Verfahrensrichtlinie zum Einsatz von IT-Verfahren im Haushalts-, Kassen- und Rechnungswesen im Land Mecklenburg-Vorpommern (VerfRi-IT-HKR)

Inhaltsverzeichnis

Erster Abschnitt: Allgemeine Bestimmungen

1. Anwendungsbereich und Zweck

1.1 Die nachfolgenden Vorschriften finden Anwendung auf IT-Verfahren für das Haushalts-, Kassen- und Rechnungswesen. Dies sind Verfahren für

- Anordnungen,
- Zahlungen,
- Geldverwaltung und Abrechnung oder
- Buchführung, Belegung der Buchungen, Abschlüsse und Rechnungslegung.

Ebenfalls zu den IT-Verfahren nach Satz 1 gehören elektronische Zahlungssysteme und IT-Verfahren, in denen Daten erzeugt und an die Verfahren nach Satz 2 zur Erfüllung der dort aufgeführten Aufgaben übergeben werden. Vor Einführung des Verfahrens ist zu prüfen, ob Bezug nehmend auf § 70 Satz 2 LHO, Anordnungen auf elektronischen Wege erteilt werden können.

1.2 Soweit beim Einsatz von IT-Verfahren einzelne Verfahrensschritte manuell erfolgen, sind auf diese Verfahrensschritte die Vorschriften für manuelle Verfahren für das Haushalts-, Kassen- und Rechnungswesen anzuwenden (Anlage 2 zu VV zu §§ 70-80 LHO).

1.3 Die nachfolgenden Vorschriften dienen der Gewährleistung der Kassensicherheit der IT-Verfahren und der Konkretisierung der Grundsätze ordnungsgemäßer Buchführung. Beim Einsatz oder bei Änderung automatisierter Verfahren im Haushalts-, Kassen- und Rechnungswesen des Landes Mecklenburg-Vorpommern sind die Bestimmungen der VV Nr. 6 zu §§ 70-80 LHO einschließlich der Anlage 6 zu VV zu §§ 70-80 LHO (GoBIT-HKR) anzuwenden. Sollen außerhalb des vom Finanzministerium betriebenen HKR-Verfahrens des Landes IT-Verfahren nach VV Nr. 6 zu §§ 70-80 LHO eingesetzt werden, so bedürfen sie der Einwilligung des Finanzministeriums (nach VV Nr. 6.6.2 zu §§ 70-80 LHO).

2. Verantwortliche Stelle

Für die Einhaltung der Bestimmungen nach VV Nr. 6 zu §§ 70-80 LHO einschließlich GoBIT-HKR und dieser Richtlinie ist der BfH der obersten Landesbehörde verantwortlich, die für den Einsatz des IT-Verfahrens zuständig ist (vgl. Nr. 2 der Anlage 6 zu §§ 70-80 LHO). Der BfH der obersten Landesbehörde kann seine Verantwortlichkeit auf einen anderen BfH übertragen. Die Übertragung der Verantwortlichkeit ist zu dokumentieren.
Bei behördenübergreifend eingesetzten IT-Verfahren ist die Behörde verantwortlich, die das Verfahren programmiert bzw. beschafft hat.
Im Rahmen des Einwilligungsverfahrens (siehe dritter Abschnitt) hat die verantwortliche Stelle die Einhaltung der Bestimmungen nach VV Nr. 6 zu §§ 70-80 LHO einschließlich GoBIT-HKR und dieser Richtlinie mit dem Antrag auf Einwilligung zu bescheinigen.

3. Unterrichtungspflichten bei Einwilligungserfordernis gemäß VV Nr. 6.6.2 zu §§ 70-80 LHO

Gemäß VV Nr. 6.6.1 zu §§ 70-80 LHO sind das FM und der LRH über beabsichtigte Verfahren nach Nr. 1.1 so **rechtzeitig** zu unterrichten, dass diese ggf. die Gestaltung der Verfahren beeinflussen können. Dabei sind seitens der nach Nr. 2 verantwortlichen Stelle auch die Möglichkeiten einer frühzeitigen Präsentation zum Funktionsumfang zu prüfen.
Das FM und der LRH sind spätestens zu Beginn der Systemtests (Test des gesamten Systems gegen die gesamten funktionalen und nicht funktionalen Anforderungen) einzubeziehen, um ggf. noch Mängel aus Sicht des Einwilligungsverfahrens auszuräumen.

Zweiter Abschnitt: Anforderungen zum Einsatz von IT-Verfahren im Haushalts-, Kassen- und Rechnungswesen

4. Grundvoraussetzungen

Die für den Einsatz des IT-Verfahrens verantwortlichen Stellen (vgl. Nr. 2) gewährleisten die Ordnungsmäßigkeit, Sicherheit und Wirtschaftlichkeit des eingesetzten Verfahrens unter Beachtung und Umsetzung der Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik in der jeweils gültigen Fassung.

Die eingesetzten Verfahren müssen die Grundvoraussetzungen der Verfahrens- und Kassensicherheit erfüllen; insbesondere sind die

- Verantwortungsabgrenzung und Verantwortungszuordnung
  (Vier-Augen-Prinzip durch Trennung der Erfassung von ermittelten zahlungsrelevanten Daten und Prüfung/Freigabe dieser Daten sowie Feststellung und Anordnung; Unveränderbarkeit festgestellter oder angeordneter Daten)
- Förmlichkeit
  (Verwendung vorgeschriebener elektronischer Schnittstellen, Aufbau der Datensätze)
- Prüfbarkeit
  (Vorhandensein und Aufbewahrung prüfbarer Unterlagen, eindeutige Zuordnung der prüfbaren Unterlagen zu den durchgeführten Zahlungen, eindeutige Zuordnung des Verursachers)
- Nachvollziehbarkeit und Dokumentation der einzelnen Verantwortungsbereiche

sicherzustellen.

Für Zwecke der Rechnungsprüfung ist der Zugriff auf das Verfahren, die Verarbeitungsschritte und die Unterlagen zu gewährleisten. Unterlagen im Sinne der Nr. 4 sind alle gemäß VV Nr. 4.7.1 zu §§ 70-80 LHO aufbewahrungspflichtigen Unterlagen.

5. Gewährleistung der Richtigkeit und Vollständigkeit der erfassten und verarbeiteten Daten

Beim Einsatz von automatisierten Verfahren im Haushalts-, Kassen- und Rechnungswesen ist die Richtigkeit und Vollständigkeit der erfassten und verarbeiteten Daten im IT-Verfahren zu gewährleisten. Dies gilt auch für die Erfassung und Änderung von Stammdaten.
Dabei ist durch organisatorische und programmtechnische Kontrollen, insbesondere durch Prüferfassung, Bildung von Kontrollsummen, Plausibilitätskontrollen und Verwendung von Prüfziffern, die Richtigkeit und Vollständigkeit der Datenerfassung und der Datenverarbeitung sicherzustellen.

5.1 Abgrenzung der Verantwortungsbereiche

5.1.1 Beim Einsatz von IT-Verfahren ist sicherzustellen, dass die Verantwortungsbereiche der am Verfahren beteiligten Personen und Stellen festgelegt und gegeneinander abgegrenzt sind (Ordnungsmäßigkeitskonzept). Berechtigungen im Verfahren dürfen nur eingerichtet werden, soweit dies zur Aufgabenerfüllung zwingend erforderlich ist (Prinzip der minimalen Berechtigung). Es ist ein Verfahren für die Verwaltung der Berechtigungen (Einrichten, Veränderung, Entzug) festzulegen. Das Verfahren muss sicherstellen, dass zu jedem Zeitpunkt festgestellt werden kann, welche Personen, einschließlich Administratoren und andere Systemverwalter, zu welchem Zeitpunkt mit welchen Berechtigungen ausgestattet gewesen sind.

5.1.2 Dokumentation der Verantwortungsbereiche

Die in dem Ordnungsmäßigkeitskonzept festgelegten Verantwortungsbereiche und Zugriffsberechtigungen sind von dem zuständigen BfH den verantwortlichen Personen zu übertragen. Die Übertragung ist zu dokumentieren. In dem IT-Verfahren muss sichergestellt sein, dass die am Geschäftsvorfall beteiligten 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.

5.1.3 Bescheinigung der Verantwortungsbereiche

Die ordnungsgemäße Wahrnehmung der Verantwortungsbereiche ist schriftlich oder auf elektronischem Wege zu dokumentieren. Aus der Bescheinigung muss erkennbar sein, welcher Verantwortungsbereich wahrgenommen worden ist.

5.1.4 Vier-Augen-Prinzip

Die zur Erfassung ermittelten zahlungsrelevanten Daten sind zur Wahrung des Vier-Augen-Prinzips von einer Person zu erfassen und von einer zweiten Person zu prüfen bzw. freizugeben.
Die Feststellung der sachlichen und rechnerischen Richtigkeit und die Ausübung der Anordnungsbefugnis sind durch zwei Personen vorzunehmen.
Ausnahmen hiervon sind nur mit Einwilligung des FM im Einvernehmen mit dem LRH zulässig (VV Nr. 1.1.2 zu §§ 70-80 LHO).

5.1.5 Trennung der Bereiche Programmentwicklung und -pflege, Abnahme und Einsatz des IT-Verfahrens

Bei IT-Verfahren sollen die Funktionen der Aufgabenerfüllung, der Verfahrensentwicklung und -pflege sowie der technischen Durchführung organisatorisch und personell getrennt werden. Die Funktionen der Aufgabenerfüllung und Verfahrensentwicklung und -pflege sind immer so zu trennen, dass eine Kumulation von risikorelevanten Befugnissen bzw. Rechten für den über das fachlich unabweisbare Maß hinausgehenden Zugriff auf schutzwürdige Datenbestände durch dieselben Personen ausgeschlossen ist.

5.2 Datenermittlung

Die Datenermittlung ist das Sammeln, Zuordnen, Verschlüsseln und die erfassungsgerechte Aufbereitung von Daten anhand von begründenden Unterlagen. Für die richtige, vollständige und rechtzeitige Ermittlung und Aufbereitung der Daten ist der zuständige Sachbearbeiter verantwortlich.

5.3 Datenerfassung

5.3.1 Datenerfassung ist die verarbeitungsgerechte Übernahme von ermittelten Daten in ein IT-Verfahren, um diese Daten weiter zu verarbeiten. Sie kann durch
manuelle oder andere Eingabe von Daten begründender Unterlagen oder
Übernahme elektronischer Daten in das IT-Verfahren erfolgen.

5.3.2 Die vollständige und ordnungsgemäße Datenerfassung, die mehrere Geschäftsvorfälle umfassen kann, ist zu bescheinigen. Mit der Bescheinigung übernimmt der Sachbearbeiter die Verantwortung für die richtige Eingabe der ermittelten Daten.

5.3.3 Wenn die sachliche und rechnerische Richtigkeit der ermittelten Daten vor der Datenerfassung nicht festgestellt wurde, übernimmt der Sachbearbeiter mit der Bescheinigung nach Nr. 5.3.2 zusätzlich die Verantwortung der Feststellung der sachlichen und rechnerischen Richtigkeit.
Der Sachbearbeiter ist auf die mit der Bescheinigung verbundene Übernahme der Verantwortung hinzuweisen.
Wird abweichend von Satz 1 die rechnerische Richtigkeit für im IT-Verfahren vollständig automatisiert erstellte Ergebnisse von Berechnungen nicht durch den Sachbearbeiter festgestellt, gilt hier die Abgabe der Erklärung der verantwortlichen Stelle (vgl. Nr. 2) über die Einhaltung der Bestimmungen nach VV Nr. 6 zu §§ 70-80 LHO einschließlich GoBIT-HKR und dieser Richtlinie im IT-Verfahren als Feststellung der rechnerischen Richtigkeit.

5.3.4 Die Datenermittlung und die Datenerfassung dürfen zusammengefasst werden.

5.4 Prüfung der erfassten Daten

5.4.1 Die erfassten Daten, insbesondere die zahlungsrelevanten Daten, sind anhand der begründenden Unterlagen von einer zweiten Person zu prüfen. Die zweite Person darf weder an der Datenermittlung noch an der –erfassung beteiligt gewesen sein (Vier-Augen-Prinzip). Das Vier-Augen-Prinzip ist durch systemtechnische Vorkehrungen zu gewährleisten.

5.4.2 Es muss gewährleistet sein, dass die prüfende Person die erfassten Daten nicht verändern kann. Werden bei der Prüfung Abweichungen zwischen den ermittelten und erfassten Daten festgestellt, müssen die Daten vor der Freigabe von einer zur Datenerfassung befugten Person berichtigt und von einer zweiten, dafür berechtigten Person erneut geprüft werden.

5.4.3 Die Prüfung der Datenerfassung ist zu bescheinigen.

5.4.4 Wurde die Buchung, Ein- oder Auszahlung vor der Prüfung nicht angeordnet, übernimmt der Prüfer mit der Bescheinigung gemäß Nr. 5.4.3 auch die Bescheinigung der Anordnungsbefugnis. Der Prüfer ist auf die mit der Übernahme verbundene Verantwortung hinzuweisen.

5.4.5 Unterstützt das automatisierte Verfahren die Datenermittlung und -erfassung durch hinreichende Plausibilitätsprüfungen und ist eine Beendigung der Dateneingabe erst nach Erledigung der automatischen Korrekturaufforderungen möglich, kann die Prüfung durch die zweite Person (Vier-Augen-Prinzip) entfallen, wenn hierfür ein anderes, dem hierdurch entstehenden Risiko angemessenes Kontrollverfahren vorgesehen ist (z.B. zufallsorientiert ausgewählte Stichproben gemäß Nr. 5.4.6).
Das durch den Verzicht auf das Vier-Augen-Prinzip verursachte Risiko für die Kassensicherheit ist in der Gefährdungsanalyse zu bewerten. Auf die VV Nr. 1.1.2 §§ 70-80 LHO wird verwiesen.

5.4.6 Stichprobenprüfung

5.4.6.1 Eine Beschränkung auf Stichproben ist ausgeschlossen bei
- Geschäftsvorfällen, die zu Zahlungen auf unbestimmte Zeit führen,
- Geschäftsvorfällen, die zu wiederkehrenden Zahlungen führen, die im voraussichtlichen Anspruchszeitraum den Betrag von 9.000 Euro übersteigen sowie
- Einmalzahlungen über 3.000 Euro
- bei dem Verzicht auf Forderungen (z.B. Niederschlagung, Erlass)
- bei Vorschusszahlungen

Für diese Fälle ist ein Stichprobenkontrollverfahren ausnahmsweise zulässig, wenn die Kassensicherheit auf andere Weise gewährleistet wird. Dies ist zu begründen und nachzuweisen.

5.4.6.2 Anforderungen an das Stichprobenkontrollverfahren

- Die Auswahl der Stichproben muss dem Zufallsprinzip folgen.
- Die Stichprobenprüfung soll vor Freigabe der zu prüfendenden Fälle zur weiteren Verarbeitung erfolgen. Das IT-Verfahren muss dabei technisch sicherstellen, dass die weitere Bearbeitung der Daten der Stichprobe bis zum Abschluss der Prüfung ausgeschlossen ist.
- Die Bestimmung der Parameter (Fehlerquote, Auswahl der Fälle etc.) muss im Hinblick auf die Gewährung der Kassensicherheit durch ein aussagekräftiges Verfahren, auf Grund von Erfahrungen oder sonstigen gesicherten Erkenntnissen erfolgen.
- Das IT-Verfahren muss die freie Einstellung der Parameter, die Auswirkungen auf die quantitative und qualitative Zusammensetzung der Stichprobe haben, ermöglichen.
- Änderungen der Parameter dürfen nur mit Zustimmung der verantwortlichen Stelle (vgl. Nr. 2) oder einer von ihm bevollmächtigten Person erfolgen.
- Wird ein Stichprobenkontrollverfahren im Rahmen eines IT-Verfahrens eingesetzt, so muss dieses auch klar in einer Dienstanweisung gegenüber den Anwendern (den Prüfern) geregelt werden.

5.4.6.3 Fehlermanagement und Berichtswesen

Für jedes Stichprobenkontrollverfahren sind ein Fehlermanagement und ein Berichtswesen einzurichten, um aus den gewonnenen Erkenntnissen über die Wirksamkeit und Wirtschaftlichkeit ggf. nötige Konsequenzen zu ziehen.
Folgende Anforderungen werden an das Fehlermanagement und das Berichtswesen gestellt:

- unverzügliche Berichtigung festgestellter Fehler
- erneute Prüfung der fehlerhaften Fälle nach Berichtigung
- Dokumentation und Auswertung der Stichprobenfälle und festgestellter Fehler
- regelmäßige Überprüfung der aufgetretenen Fehlerkonstellationen, um ggf. die Ausgestaltung des Stichprobenkontrollverfahrens zu ändern, sowie Dokumentation der Prüfung

5.5 Datenverarbeitung

5.5.1 Nach Prüfung dürfen die Daten zur weiteren Verarbeitung freigegeben werden. Die Prüfung und die Freigabe der Daten können zusammengefasst werden. Eine Änderung der geprüften Daten muss ausgeschlossen sein.
Es muss systemtechnisch sichergestellt sein, dass die Freigabe unter Angabe der freigebenden Person, das Datums und der Uhrzeit eindeutig, dauerhaft und unveränderlich dokumentiert wird.

5.5.2 Stellt sich die Unrichtigkeit der Daten erst nach der Freigabe heraus, sind die Daten unverzüglich zu ändern oder zu stornieren. Die nachträglichen Änderungen oder Stornierungen unterliegen in einem erneuten Anordnungsverfahren den Grundsätzen der Nr. 5.3 Datenerfassung, der Nr. 5.4 Prüfung der erfassten Daten sowie der Nr. 5.5 Datenverarbeitung.

5.5.3 Es ist sicherzustellen, dass bereits verarbeitete Daten nicht erneut verarbeitet werden und es nicht zu Mehrfachzahlungen bzw. –buchungen kommt.

5.6 Zugangs- und Zugriffskontrollen

5.6.1 Beim Einsatz von IT-Verfahren ist sicherzustellen, dass eine Zugangs- und Zugriffskontrolle gewährleistet ist und in den Arbeitsablauf nicht unbefugt eingegriffen werden kann.

5.6.2 Der Zugriff auf das Verfahren ist durch ein Passwort zu schützen.

5.6.3 Zugriffe auf das Verfahren sind zu dokumentieren.

5.7 Nachweis von Datenbestandsveränderungen

Bei Einsatz eines IT-Verfahrens müssen sämtliche Erfassungen und Veränderungen der Daten an Hand geeigneter Maßnahmen nachgewiesen werden (z.B. anhand einer Datenbankfunktion, Protokolldatei oder eines Verarbeitungsprotokolls). Der Nachweis muss

- den eindeutig gekennzeichneten Geschäftsvorfall,
- das Datum, die Uhrzeit und die Benutzerkennung des Sachbearbeiters, der die Erfassung bzw. Änderung vorgenommen hat sowie
- die erfassten und geänderten Daten mit altem und neuem Stand

enthalten.

5.8 Revisionsfähigkeit des Verfahrens

5.8.1 IT-Verfahren sind so auszugestalten, dass über sämtliche buchführungspflichtige Geschäftsvorfälle für die Dauer der Aufbewahrungspflicht (vgl. VV Nr. 4.7 i.V.m. Nr. 6 der Anlage 6 zu §§ 70-0-80 LHO) ein sachlicher und zeitlicher Nachweis erbracht werden kann. Dieser muss von einer sachverständigen, nicht am Verfahren beteiligten Person in angemessener Zeit dahingehend prüfbar sein, ob

- die verfahrensrechtlichen Vorgaben der Bestimmungen nach VV Nr. 6 zu §§ 70-80 LHO einschließlich GoBIT-HKR und dieser Richtlinie eingehalten wurden (formelle Richtigkeit) und
- die inhaltlichen Anforderungen an eine Buchung sowie an eine Ein- bzw. Auszahlung, insbesondere das Vorliegen eines Rechtsgrundes, erfüllt sind (materielle Richtigkeit).

Die Geschäftsvorfälle müssen retrograd und progressiv prüfbar sein, das heißt, der Zusammenhang zwischen erfassten und verarbeiteten Daten bis zur Buchung muss sowohl von der Datenerfassung ausgehend chronologisch fortschreitend (progressiv) als auch von der Buchung ausgehend chronologisch rückschreitend (retrograd) erkennbar und nachvollziehbar sein. Erfolgt die Dokumentation nicht bereits bei der Datenerfassung oder -übernahme, sondern erst auf einer nachfolgenden Verarbeitungsstufe, dann ist durch Kontrollen oder andere Maßnahmen die Vollständigkeit der Geschäftsvorfälle von deren Entstehung bis zu deren Dokumentation sicherzustellen.

5.8.2 Die durch das IT-Verfahren vorgenommenen Buchungen und ihre Reihenfolge sind durch Belege (Nachweise über Buchungen) zu dokumentieren. Zu jedem Buchungsvorgang sind die folgenden Informationen nachzuweisen:

- hinreichende Erläuterung des Vorgangs,
- zu buchender Betrag,
- den Zahlungspartner mit den für den Zahlungsverkehr notwendigen Angaben,
- Zeitpunkt des Vorgangs und
- die gemäß Nr. 5.1.3 erfolgten Bescheinigungen.

Gehören zum Beleg begründende Unterlagen ist zu gewährleisten, dass sowohl die begründenden Unterlagen dem Beleg als auch die Belege den begründenden Unterlagen eindeutig zugeordnet werden können.

5.8.3 Die Belege müssen nach ihrer Erstellung unveränderbar sein und lesbar gemacht werden können. Die Darstellung der Geschäftsvorfälle muss vollständig oder auszugsweise sowie geordnet nach Zeitpunkt, Sach- und Personenkonten erfolgen können.

5.8.4 Die Prüfbarkeit der formellen und materiellen Richtigkeit hinsichtlich der Revisionsfähigkeit des Verfahrens bezieht sich sowohl auf einzelne Geschäftsvorfälle (Einzelprüfung) als auch auf die Prüfbarkeit des gesamten Verfahrens (Verfahrens- oder Systemprüfung anhand einer Verfahrensbeschreibung).

5.8.5 Im IT-Verfahren sind Berechtigungen (z.B. eine vordefinierte Prüferrolle) einzurichten, die durch direkte Zuordnung zu einer Person einen lesenden Zugriff auf alle Daten und Systemeinstellungen des IT-Verfahrens ermöglichen.

5.9 IT-Sicherheit

5.9.1 IT-Verfahren dürfen nur eingesetzt werden, wenn hinreichende Vorkehrungen gegen den Verlust und die Manipulation gespeicherter Daten (Dateien und Verarbeitungsprogramme) durch unberechtigte Dritte sowie gegen Systemfehler getroffen sind.

5.9.2 Die Regelungen im IT-Grundschutzkatalog des BSI gelten unmittelbar (VV Nr. 6.1.2 zu §§ 70-80 LHO).
Durch die verantwortliche Stelle (vgl. Nr. 2) ist zu bestätigen, dass ein Sicherheitskonzept gemäß IT-Grundschutz einschließlich ergänzender Bestimmungen des BSI in aktueller Form vorliegt und umgesetzt wird.

5.9.3 Test- und Freigabeverfahren

Zur Wahrung der Integrität der Daten darf beim Einsatz eines IT-Verfahrens nur dokumentierte und nach einem erfolgreichen Testverfahren durch eine bevollmächtigte Person freigegebene Software eingesetzt werden.

5.9.4 Es ist durch den Abschluss von Wartungsverträgen oder auf andere Weise sicherzustellen, dass entstehende oder sichtbar werdende Programmfehler oder Sicherheitslücken in angemessener Zeit beseitigt werden.

5.10 Internes Kontrollsystem

Mit der Einführung von IT-Verfahren ist sicherzustellen, dass die Einhaltung der Bestimmungen nach VV Nr. 6 zu §§ 70-80 LHO einschließlich GoBIT-HKR und dieser Richtlinie regelmäßig überprüft wird. Dabei ist auch zu kontrollieren, ob das eingesetzte IT-Verfahren dem dokumentierten und genehmigten Verfahren entspricht (Programmidentität). Erforderlich sind sowohl systemtechnische als auch manuelle Kontrollen. Der Höchstzeitraum zwischen den Kontrollen ist ausgehend von der Eintrittswahrscheinlichkeit des durch das IT-Verfahren verursachten Risikos für die Kassensicherheit festzulegen. Unabhängig von der Eintrittswahrscheinlichkeit muss eine Kontrolle des IT-Verfahrens und seiner Anwendung in festgelegten Mindestabständen erfolgen.
Es ist eine verantwortliche Person für die regelmäßigen und anlassbezogenen Kontrollen zu benennen.

6. Elektronische Schnittstellen zum HKR-Verfahren und Zahlungsverkehrsverfahren des Landes

Bei der Datenfernübertragung von Zahlungsverkehrs-, Buchungs- und Anordnungsdaten über eine elektronische Schnittstelle zwischen IT-Verfahren und dem HKR-Verfahren bzw. dem Zahlungsverkehrsverfahren des Landes muss gewährleistet sein, dass

- die Daten unverändert und vollständig gesendet und empfangen werden,
- die Übertragung von Daten wiederholt werden kann und
- die Daten von Sende- und Empfangsdateien visuell lesbar gemacht werden können.

6.1 Datenübertragung

Bei der Übermittlung bzw. Entgegennahme von Zahlungsverkehrs-, Buchungs- und Anordnungsdaten über eine elektronische Schnittstelle zum/vom HKR-Verfahren oder Zahlungsverkehrsverfahren ist eine nach dem Stand der Technik sichere Methode der Datenübertragung zu wählen.

6.1.1 Für IT-Verfahren, die nicht im DVZ betrieben werden, ist das Transportprotokoll OSCI (XTA) zu verwenden.

6.1.2 Gemäß dem zwischen der DVZ und dem FM geschlossenen Dienstleistungsvertrag werden die Kosten für die Erstinstallation sowie die laufenden Kosten für die Datenübertragung vom FM getragen.

6.1.3 Kontrollmechanismen

Die Verwendung vorgegebener Transportprotokolle soll neben der Sicherheit auch die Vollständigkeit der Datentransporte gewährleisten.
Die Hinweise des DVZ an die Teilnehmer der Verfahren Profiskal und CBPay zur technischen Abwicklung der Datentransporte (Anlage 1) sind zwingend zu beachten.
Bei Vorliegen eines Datentransferproblems sind die entsprechenden Formulare zur Fehlermeldung (Anlagen 2 und 3) zu verwenden.

6.2 Schnittstelle zum HKR Verfahren ProFiskal

Das HKR-Verfahren ProFiskal verfügt über eine Batch-Input-Schnittstelle über die Buchungs- und Quittungsdateien im ASCII-Format ausgetauscht werden können.
Die Schnittstellenbeschreibung wird durch das FM bereitgestellt.

6.3 Schnittstelle zum Zahlungsverkehrsverfahren CBPay

Bei der Anlieferung von Zahlungsdateien an das Zahlungsverkehrsverfahren haben diese Dateien der Schnittstellenspezifikation zum „Abkommen über die Datenfernübertragung zwischen Kunde und Kreditinstitut“ (DFÜ-Abkommen) zu genügen.

Die Datensatzbeschreibung ist der „Anlage 3 der Schnittstellenspezifikation für die Datenfernübertragung zwischen Kunde und Kreditinstitut gemäß DFÜ-Abkommen“ „Spezifikation der Datenformate“ in der aktuellen Version zu entnehmen.

Näheres zur Spezifikation der Datenformate sowie zu den Bestimmungen zur Anlieferung der Zahlungsdateien und der Zahlungsbegleitinformation regelt das FM mit gesonderten Erlassen.

6.4 Prüfung/Test der elektronischen Schnittstellen auf Ordnungsmäßigkeit

Vor dem erstmaligen Einsatz eines IT-Verfahrens und bei technischen und/oder organisatorischen Änderungen eines bereits eingesetzten IT-Verfahrens, die Auswirkungen auf die Buchungs-, Anordnungs- bzw. Zahlungsdaten haben, sind die Buchungs-, Anordnungs- bzw. Zahlungsdaten auf ihre Verarbeitungsfähigkeit zu prüfen.

Die fachliche und technische Prüfung und Freigabe des IT-Verfahrens (geeignetes Test- und Freigabeverfahren zur Wahrung der Programmidentität) bleibt hiervon unberührt.

Bei der Übergabe von Testdateien sind keine Echtdaten zu verwenden.

6.4.1 Batch-Input-Test

Die Batch-Input-Schnittstelle „Fachverfahren <-> ProFiskal“ ist bei neu einzuführenden IT-Verfahren im vollen Funktionsumfang und bei geänderten IT-Verfahren im Hinblick auf die vorgenommenen Änderungen zu testen.

Die für die Durchführung der Testung verantwortliche Stelle unterrichtet das FM rechtzeitig über anstehende Tests. Der Grund bzw. Zweck des Tests (z.B. Neueinführung, Erweiterung des Funktionsumfangs, Hard- oder Softwarewechsel etc.), der Umfang der Testarbeiten, der gewünschte Testzeitraum sowie die entsprechenden fachlichen Ansprechpartnern sind zu benennen. Das FM informiert zwecks Abstimmung und Planung der Testarbeiten die LZK und das DVZ.

Die LZK erteilt nach Beendigung der entsprechenden erfolgreichen Testarbeiten eine abschließende Testbescheinigung.

6.4.2 Test Schnittstelle Zahlungsverkehrsverfahren

Die Schnittstelle „Fachverfahren <-> CBPay“ ist bei neu einzuführenden IT-Verfahren und ggf. bei geänderten IT-Verfahren im Hinblick auf die vorgenommenen Änderungen zu testen.

Die für die Durchführung der Testung verantwortliche Stelle unterrichtet das FM rechtzeitig über anstehende Tests. Der Grund bzw. Zweck des Tests (z.B. Neueinführung, Erweiterung des Funktionsumfangs, Hard- oder Softwarewechsel etc.), der Umfang der Testarbeiten, der gewünschte Testzeitraum sowie die entsprechenden fachlichen Ansprechpartnern sind zu benennen. Das FM informiert zwecks Abstimmung und Planung der Testarbeiten die LZK und das DVZ.
Die für die Durchführung der Testung verantwortliche Stelle übersendet die entsprechenden Testdaten an das FM.

Das FM erteilt nach Beendigung der entsprechenden erfolgreichen Testarbeiten eine abschließende Testbescheinigung.

7. Nachweis der Einhaltung der geltenden Bestimmungen

7.1 Die nach Nr. 2 verantwortliche Stelle hat die Einhaltung der Bestimmungen nach VV Nr. 6 zu §§ 70-80 LHO einschließlich GoBIT-HKR und dieser Richtlinie nachzuweisen.

7.2 Der Nachweis erfolgt im Falle der Einführung von IT-Verfahren durch Vorlage

- der Verfahrensdokumentation
- der Gefährdungsanalyse
- des Ordnungsmäßigkeitskonzepts
- der Prüfliste

Inhalt und Aufbau der Unterlagen können den anliegenden Musterunterlagen entnommen werden.

7.3 Im Falle einer Änderung von genehmigten IT-Verfahren erfolgt der Nachweis zusätzlich durch eine Beschreibung der Änderung und Analyse der mit der Änderung verbundenen Risiken.

7.4 Ergänzende Bestimmungen zu den erforderlichen Unterlagen

7.4.1 Verfahrensdokumentation

Die Verfahrensdokumentation beschreibt den organisatorisch und technisch gewollten Prozess, z.B. bei elektronischen Dokumenten von der Information über die Indizierung, Verarbeitung und Speicherung, dem eindeutigen Wiederfinden und der maschinellen Auswertbarkeit, der Absicherung gegen Verlust und Verfälschung und der Reproduktion. Für den Zeitraum der Aufbewahrungsfrist muss gewährleistet sein, dass das in der Dokumentation beschriebene Verfahren dem in der Praxis eingesetzten Verfahren voll entspricht. Dies gilt insbesondere für die eingesetzten Versionen der Programme (Programmidentität). Die Verfahrensdokumentation ist bei Änderungen zu versionieren und eine nachvollziehbare Änderungshistorie vorzuhalten.

Inhalt und Aufbau der Verfahrensdokumentation können der anliegenden Musterunterlage entnommen werden.

7.4.2 Gefährdungsanalyse

In der Gefährdungsanalyse ist insbesondere darzulegen,
- welche durch das IT-Verfahren verursachten Risiken bestehen und welche Sicherheitsmaßnahmen zur Risikoverringerung vorgesehen sind,
- wie hoch die verbleibenden Eintrittswahrscheinlichkeiten der Risiken sind und zu welchen Vermögensschäden der Eintritt führen würde und
- aus welchen Gründen auf weitergehende Schutzmaßnahmen verzichtet wird.

Inhalt und Aufbau der Gefährdungsanalyse können der anliegenden Musterunterlage entnommen werden.

7.4.3 Ordnungsmäßigkeitskonzept

Inhalt und Aufbau des Ordnungsmäßigkeitskonzeptes können der anliegenden Musterunterlage entnommen werden.

7.4.4 Prüfliste

Inhalt und Aufbau der Prüfliste können der anliegenden Musterunterlage entnommen werden.

7.4.5 Die in Nr. 7.2 und Nr. 7.3 genannten Dokumente ersetzen nicht die nach anderen Vorschriften vorgeschriebenen Dokumentationen (z.B. Sicherheitskonzepte nach BSI, Wirtschaftlichkeitsbetrachtungen, Verfahrensbeschreibung, Arbeitsanweisung für den Anwender etc.), sondern dienen lediglich dem Nachweis der Einhaltung der Bestimmungen nach VV Nr. 6 zu §§ 70-80 LHO einschließlich GoBIT-HKR und dieser Richtlinie.

Dritter Abschnitt: Einwilligungsverfahren

8. Einwilligungserfordernis und Antragstellung

8.1 Einführung neuer IT-Verfahren

IT-Verfahren im Haushalts-, Kassen- und Rechnungswesen (vgl. Nr. 1.1) bedürfen vor ihrer Einführung der Einwilligung des FM im Einvernehmen mit dem LRH.
Dies gilt auch für IT-Verfahren, die über keine elektronische Schnittstelle zum HKR-Verfahren verfügen.

8.2 Änderung von IT-Verfahren

Die Änderung bereits eingewilligter, produktiver IT-Verfahren bedarf nur dann der Einwilligung das FM, wenn die Änderung zu einer Abweichung von den Bestimmungen nach VV Nr. 6 zu §§ 70-80 LHO einschließlich GoBIT-HKR und dieser Richtlinie führt (z.B. Änderungen im Ablauf des Anordnungsverfahrens), die nicht von einer bereits erteilten Genehmigung des FM erfasst ist. Eine Änderung des IT-Verfahrens liegt auch dann vor, wenn ausschließlich manuelle Verfahrensschritte verändert werden.

Die beim Inkrafttreten der VV zu §§ 70-80 LHO (Stand 06/2016) und dieser Vorschriften in Betrieb befindlichen genehmigten Verfahren müssen die sich hieraus ergebenden Vorgaben spätestens dann erfüllen, wenn eine maschinelle Schnittstelle zum HKR-Verfahren oder Zahlungsverkehrsverfahren des Landes eingerichtet oder das IT-Verfahren wesentlich geändert wird.

8.3 Antragstellung

Die Erteilung der Einwilligung für die Einführung eines IT-Verfahrens ist von der nach Nr. 2 verantwortlichen Stelle mindestens fünf Monate vor der geplanten Einführung nach folgender Maßgabe beim FM zu beantragen.

Die Erteilung der Einwilligung für die Änderung eines IT-Verfahrens ist von der nach Nr. 2 verantwortlichen Stelle mindestens drei Monate vor der geplanten Umsetzung der Änderung nach folgender Maßgabe beim FM zu beantragen.

Der Antrag muss
- die Bescheinigung der verantwortlichen Stelle (vgl. Nr. 2) über die Einhaltung der Bestimmungen nach VV Nr. 6 zu §§ 70-80 LHO einschließlich GoBIT-HKR und dieser Richtlinie
- die nach Nr. 7.2 sowie Nr. 7.3 erforderlichen Unterlagen

enthalten.

Für die Antragstellung ist der entsprechende Vordruck (Anlage 4) zu verwenden.

9. Prüfungsverfahren und Einwilligung

9.1 Das FM prüft die mit dem Antrag eingereichten Unterlagen auf Einhaltung der Bestimmungen nach VV Nr. 6 zu §§ 70-80 LHO einschließlich GoBIT-HKR und dieser Richtlinie. Bei Abweichungen werden die Voraussetzungen für die Erteilung einer Ausnahmegenehmigung geprüft.

9.2 Das FM ist für die Herstellung des Einvernehmens mit dem LRH verantwortlich. Hierzu werden die durch das FM geprüften Unterlagen an den LRH übergeben.

9.3 Eine Produktivstellung des neuen bzw. geänderten IT-Verfahrens ist erst nach erteilter Einwilligung zulässig.

9.4 Das FM kann die Einwilligung entziehen, wenn es auf Grund nachträglich eingetretener oder bekannt gewordener Tatsachen berechtigt wäre, die Einwilligung nicht zu erteilen. In diesem Fall entscheidet das FM, ob und unter welchen Voraussetzungen das IT-Verfahren in Zukunft ohne Einwilligung genutzt werden darf.

10. Pflichten nach Abschluss des Einwilligungsverfahrens

10.1 Kontrollen und Risikoprüfung

Während des Einsatzes von IT-Verfahren ist die Einhaltung der Bestimmungen nach VV Nr. 6 zu §§ 70-80 LHO einschließlich GoBIT-HKR und dieser Richtlinie regelmäßig durch die nach Nr. 2 verantwortliche Stelle zu prüfen (vgl. auch Nr. 10.3). Dies schließt insbesondere die Prüfung ein, ob die erstellte Gefährdungsanalyse weiterhin zutreffend ist. Werden Verstöße gegen die Bestimmungen nach VV Nr. 6 zu §§ 70-80 LHO einschließlich GoBIT-HKR und dieser Richtlinie festgestellt, sind unverzüglich Maßnahmen dagegen zu ergreifen.

10.2 Nachträgliche Änderung von IT-Verfahren

Die Änderungen im IT-Verfahren sind in den gemäß Nr. 7 erforderlichen Dokumenten nachzuweisen. Dies gilt unabhängig davon, ob ein Einwilligungserfordernis besteht.
Das geänderte IT-Verfahren ist fachlich und technisch zu prüfen und freizugeben (geeignetes Test- und Freigabeverfahren zur Wahrung der Programmidentität).

10.3 Vordruck Erhebungsbogen IT-Verfahren

Die verantwortlichen Stellen (vgl. Nr. 2) für IT-Verfahren, für die bereits die Einwilligung des FM erteilt wurde, haben in einer jährlichen Berichtspflicht bis zum 30.03. des Jahres den Vordruck „Erhebungsbogen IT-Verfahren“ (Anlage 5) an das FM zu übergeben.
Die Richtigkeit der Angaben ist durch die verantwortliche Stelle (vgl. Nr. 2) zu bestätigen. Auf die in diesem Zusammenhang bestehende Ressortverantwortung wird ausdrücklich hingewiesen.

Anlagenverzeichnis

Anlage 1	Hinweise des DVZ an die Teilnehmer der Verfahren Profiskal und CBPay zur technischen Abwicklung der Datentransporte
Anlage 2	Formular Meldung Datentransferproblem für ProFiskal
Anlage 3	Formular Meldung Datentransferproblem für CBPay
Anlage 4	Antrag auf Einwilligung gemäß VV Nr. 6.6 zu §§ 70-80 LHO M-V
Anlage 5	Vordruck Erhebungsbogen IT-Verfahren HKR

Muster

Verfahrensdokumentation
Gefährdungsanalyse
Ordnungsmäßigkeitskonzept
Prüfliste

Abkürzungsverzeichnis

LHO	Landeshaushaltsordnung M-V
BfH	Beauftragte(r) für den Haushalt
VV	Verwaltungsvorschrift zur Landeshaushaltsordnung M-V
FM	Finanzministerium M-V
LRH	Landesrechnungshof M-V
LZK	Landeszentralkasse M-V
DVZ	Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
BSI	Bundesamtes für Sicherheit in der Informationstechnik

THEMA:

Hinweise an die Teilnehmer der Verfahren Profiskal und CBPay zur technischen Abwicklung der Datentransporte

AUFTRAGGEBER:

Finanzministerium
des Landes Mecklenburg-Vorpommern

DATUM:

22.03.2017

VERSION:

0.9

DVZ Datenverarbeitungszentrum
Mecklenburg-Vorpommern GmbH

1 ALLGEMEINES

Zur Abwicklung der Geschäftsprozesse beim Kassenverfahren (CBPay) und der Haushaltsrechnung (Profiskal) ist es notwendig, dass die Teilnehmer am Verfahren ihre Daten an CBPay bzw. Profiskal mittels netzwerktechnischer Kommunikationsprozesse übertragen und (in der Regel) auch entsprechende fachliche Ergebnisdaten auf gleichem Weg zurück erhalten. Diese Kommunikation erfolgt über verschiedene Netzwerke und Serversysteme hinweg. Entsprechend den technischen, organisatorischen und sicherheitstechnischen Gegebenheiten und Erfordernissen, haben sich zum Datentransport unterschiedliche Lösungen etabliert. Allen sind jedoch die nachfolgend dargestellten Grundsätze und Regeln gemein, die zwingend einzuhalten sind.

Neben der Sicherheit (Nichteinsehbarkeit für Dritte) ist die Vollständigkeit der Datentransporte (Teilnehmer vs. CBPay/Profiskal) ein essentielles Ziel. Störungen seitens des Netzwerkes, der beteiligten Server und Softwaresysteme können nicht vollständig ausgeschlossen werden. Aus diesem Grund sind bestimmte Kontrollmechanismen in den Prozess integriert worden, die unter dem Stichwort „Quittungsmechanismus“ zusammengefasst sind.

Für das Verständnis der Kommunikationsabläufe sollen die nachfolgenden Grafiken illustrieren, welche Systeme an der Kommunikation beteiligt sind. Abbildung 1 stellt den prinzipiellen Ablauf beim Datentransport zwischen Verfahrensteilnehmern und den Verfahren CBPay/Profiskal dar. Wesentliches Element des Datentransportes ist es, dass die Teilnehmer an der Kommunikation nicht direkt mit den Verfahren CBPay/Profiskal kommunizieren, sondern dies über die als „**Postfachserver**“ bezeichnete Serverkomponente realisieren. Eine gewisse Abweichung/Sonderstellung haben die Datentransporte, bei denen die Teilnehmer nicht im internen Netzwerk des DVZ (Rechenzentrumsnetzwerk) verortet sind. Hier erfolgt der Transport vom Teilnehmer zum Postfachserver über das Protokoll OSCI. Diese Kommunikation wird über ein weiteres Server-System (OSCI-Intermediär/Virtuelle Poststelle) abgewickelt. In Abbildung 1 ist der schematische Ablauf für Datentransporte dargestellt. Der OSCI-Intermediär ist gestrichelt angegeben, um kenntlich zu machen, dass zu diesem Protokoll spezifische Gegebenheiten vorliegen. Eine detaillierte Darstellung zu OSCI ist im Anhang 2 zu finden.

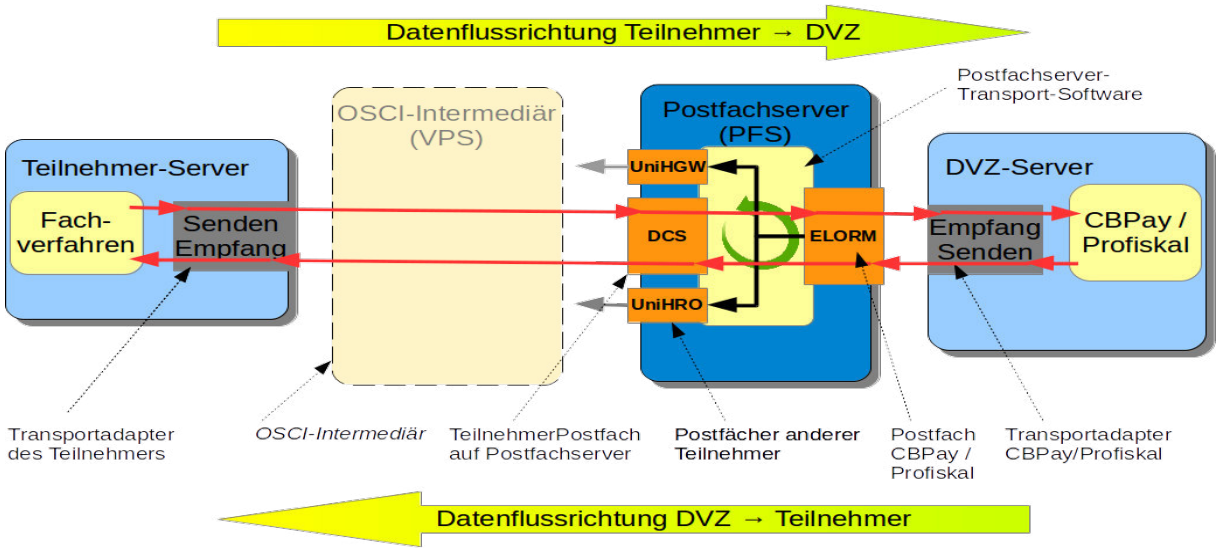

Abbildung 1: Schema der Datentransporte von/zu CBPay/Profiskal

2 TECHNISCHE VERSANDQUITTUNGEN

2.1 Ablauf und Aufbau des Quittungsmechanismus

In der Vergangenheit hat sich die Anlieferung von Daten seitens der Teilnehmer als kritischer Punkt in der Gesamtkommunikation zwischen den Verfahren CBPay und Profiskal auf der einen Seite sowie allen teilnehmenden Verfahren auf der anderen Seite erwiesen. Die Teilnehmer an der Kommunikation haben entweder keine oder nur unzureichende/unsichere Kontrolle darüber, ob die von ihnen versendeten Daten auf dem Postfachserver auch wirklich angekommen sind.

Zur Beseitigung dieses Informationsdefizites erstellt der Postfachserver zu jeder bei ihm eingetroffenen Nachricht, die die Kriterien zur erfolgreichen Weiterleitung an den Empfänger erfüllt, eine entsprechende Quittungsdatei. Diese Quittungsdatei dokumentiert auf der technischen Ebene, dass der Teilnehmer seine Daten erfolgreich an den Postfachserver übermittelt hat. Nachfolgende Grafik illustriert den Ablauf der Quittungserstellung im Prozess der Datenübermittlung.

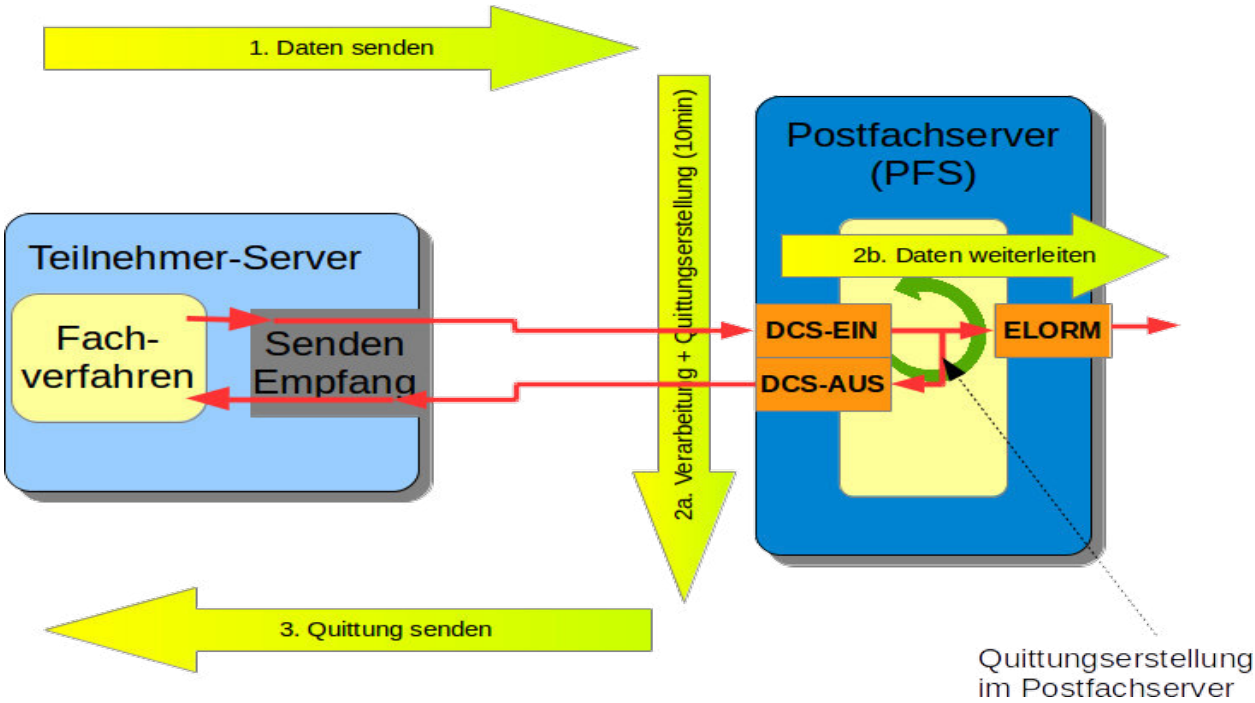

Abbildung 2: Schema der Quittungserstellung

Diese Quittungsdatei ist die Eingangsbestätigung am Postfachserver. Sie attestiert dem Absender, dass seine Daten auf dem Postfachserver angekommen sind und das die Daten in die Weiterleitung zum gewünschten Empfänger gegeben wurden. Diese Quittung attestiert jedoch nicht, dass die Daten beim Endempfänger angekommen sind und natürlich bzw. dass die Daten in das Fachverfahren des Endempfängers korrekt verarbeitet wurden. Es ist lediglich eine technische und keine fachliche Quittung. Die Quittungsdatei wird vom Postfachserver für den datenanliefernden Teilnehmer des Verfahrens bereitgestellt.

Dabei lautet der Dateiname der Quittung wie folgt: **Quittung_[NameDerÜbermitteltenDatei]**
Beispiel:

- angelieferte Datei lautet: PRO_testverfahren_BAI121216-34450001-2.inp
- erstellte Quittung lautet : Quittung_ PRO_testverfahren_BAI121216-34450001-2.inp

In jeder Quittungsdatei selbst sind Angaben über die Datenlieferung des Teilnehmers hinterlegt. Diese Daten beziehen sich nicht auf den fachlichen Inhalt, sondern auf die technischen Metadaten der angelieferten Datei. Nachfolgend ist die Liste der Dateieigenschaften/Attribute angegeben:

1. Kopf der Quittungsdatei
2. Metadaten der empfangenen Datei
    a. Dateiname
    b. Dateigröße
    c. Datum und Uhrzeit des Empfangs (Auffindezeitpunkt durch Postfachserver-Software)
    d. Checksumme über den Dateiinhalt (sha256)
3. Der öffentliche Zertifikatsschlüssel zur Signatur des Hashwertes der Datei
4. Signatur der Datei, die zum Hashwert erstellt wurde
5. Hinweis zur Prüfung der Signatur (falls notwendig)
6. Abschlusszeile

Im Anhang-1 finden Sie ein exemplarisches Beispiel für eine solche Quittungsdatei.

2.2 Umgang mit Quittungsdateien

Es wird im Sinne der Stabilität des Transportprozesse empfohlen, die Quittungsdateien auszuwerten. Um auch eine automatische Auswertung der Quittungen zu ermöglichen, beginnen die einzelnen Abschnitte 1. bis 4. der oben stehenden Inhaltsliste der Quittungsinhalte stets an der selben Stelle/Zeile. Beachten Sie dabei, dass nicht nur die Prüfung auf Identität des Dateinamens zu erfolgen hat, sondern mindestens auch auf Identität der Dateigröße. Die Prüfung auf die Checksumme dient einem schnellen Test der Unversehrtheit der Daten bei der Übertragung. Stimmt die Checksummen in der Quittung nicht mit der Checksumme auf Ihrem System überein, sind die Daten entweder durch einen technischen Übertragungsfehler oder absichtlich durch Dritte verfälscht worden. Die Prüfung der Signatur stellt den vollumfänglichen Test auf Unversehrtheit der übertragenen Daten dar.

Die Quittungsdateien sind für Sie der Nachweis, dass Sie Ihren Pflichten bei der Datenlieferung korrekt nachgekommen sind. Sie sollten Sie entsprechend der für Sie geltenden Aufbewahrungsfristen zusammen mit den Originaldaten archivieren. Sollten keine Fristen bekannt oder definiert worden sein, ist unsere Empfehlung die Daten mindestens 6 Monate lang zu speichern. Beachten Sie, dass in der Regel auch eine maximale Archivierungsfrist existiert.

Quittungen zu Datensendungen werden vom Postfachserver zum Zeitpunkt ausgestellt, in dem die Daten an den Empfänger zur Abholung/Übertragung übermittelt werden. Diese Quittungen werden unmittelbar an den datenübermittelnden Teilnehmer (zurück-)gesendet bzw. zur Abholung bereitgestellt. Das Eintreffen der Quittungen hängt vom genutzten Übertragungsprotokoll sowie von den konkreten zeitlichen Einstellungen auf den beteiligten Softwarekomponenten ab (z. B. Sende-/Abholzyklen) ab. Die konkreten Zeiten zwischen Versand der Fachdaten und dem Eintreffen der zugehörigen Quittung können somit variieren. Zur Überprüfung des ordnungsgemäßen Ablaufs von Datenversand und Quittungsempfang muss jeder Teilnehmer Kenntnis über die Dauer eines solchen Zyklus an seinem System haben bzw. ermitteln.

3 STÖRUNGEN BEIM DATENTRANSPORT

3.1 Vorgehen im Störungsfall (Aufgaben für DVZ und Teilnehmer)

Sollte in dem erwarteten Zeitraum für das Eintreffen einer Quittung diese nicht beim Teilnehmer vorliegen, ist dies ein erster Hinweis darauf, dass die Übertragung auf irgendeine Weise gestört ist, bzw. ein beteiligtes System ganz ausgefallen ist. In diesem Fall hat der betroffene Teilnehmer wie folgt vorzugehen:

1. Überprüfen Sie, ob die zu versendende Datei tatsächlich Ihr System verlassen hat.
   Bei Netzwerkstörungen oder Störungen im Transportprotokoll sollte die entsprechende Datei immer noch in Ihrem „Ausgabe-Verzeichnis“ liegen.
   Wenn dies der Fall ist, sollten Sie den Versand manuell auslösen, um sicherzustellen, dass das Problem nicht ggf. im Aufruf (bzw. Nicht-Aufruf) Ihrer Versandkomponente liegt.
   Können Sie einen Fehler auf Ihrem System ausschließen und die Daten dennoch nicht versenden, geben Sie ein Störungsticket (Incident) beim ServiceDesk des DVZ unter servicedesk@dvz-mv.de (Tel.: 0385/4800 565) auf.
2. Wenn Sie sicher sind, dass Ihre Datei versendet wurde und die Quittung nicht bei Ihnen im erwarteten Zeitfenster eingetroffen ist, müssen Sie zunächst das vom Finanzministerium im Zuge des Einwilligungsverfahrens übermittelte Störungsformular zum „Vorliegen eines Datentransferproblems“ ausfüllen. Insbesondere ist der Dateiname anzugeben, zu der Sie keine Quittung erhalten haben. Auch in diesem Fall geben Sie ein Störungsticket beim ServiceDesk des DVZ unter servicedesk@dvz-mv.de (Tel.: 0385/4800 565) auf. Fügen Sie Ihrer Störungsmeldung das genannte Störungsformular bei.
3. Beim Ausbleiben einer fachlichen Antwort des Verfahrens Profiskal (CBPay erzeugt keine fachlichen Antworten) an Sie, müssen Sie ebenfalls das genannte Formular ausfüllen, allerdings ohne dass Sie hier angeben können, welche Datei Ihnen fehlt. Dies ergibt sich dann aus den sonstigen Angaben, die im Formular abgefragt werden. Gehen Sie ansonsten wie unter 2. beschrieben vor.

4. Nach Eintreffen Ihrer Störungsmeldung bei unserem ServiceDesk wird Ihr Ticket der Fachabteilung für die Verfahren CBPay/Profiskal zugewiesen. Falls notwendig, wird der von Ihnen auf dem Formular angegebene Ansprechpartner zu Rückfragen kontaktiert. Beachten Sie bitte, dass die Störungsbeseitigung ohne Angabe eines Ansprechpartners bzw. der sonstig geforderten Angaben nicht begonnen werden kann und sich somit entweder stark verzögern kann oder gar zurückgewiesen wird.
5. Nach Eingang Ihrer Störungsmeldung wird der Fall entsprechend der nachfolgenden SLA-Zeiten bearbeitet:
   Service-Zeiten: Mo.-Do.: 08:00 - 17:00 Uhr
   Fr.: 08:00 - 15:00 Uhr
   (Hinweis: Die Servicezeit = Zeitraum, in dem die Störungsbeseitigung realisiert werden kann)
6. Nach Abschluss der Störungsbeseitigung erhalten Sie vom ServiceDesk eine Meldung mit dem Ergebnis der Arbeiten.

4 ANHANG

4.1 Anhang 1: (Beispiel einer Quittungsdatei)

```
Quittungsdatei des DVZ-Postfachserver vom : Fr 20. Mai 07:47:50 CEST 2016 (Systemzeit)

Ausgestellt auf die empfangene Datei, mit folgenden Attributen:
Dateiname         : PRO_elorm_SEPA.BAFOEG.CCT.20160219001058
Dateigröße        : 10157639 (Byte)
Empfangen am      : 2016-05-20 07:47:50.000000000 +0200
Checksumme sha256 : 746f70ac7d357470e7f7cae4361d73b7ca0403d41c5cecac9e2208d74175bc42 -

Erstellt mit Schlüsselmaterial aus der DOI-CA (ehemals Testa)-->Zertifikat:
-----BEGIN CERTIFICATE-----
MIIFrTCCBJWgAwIBAgIHAqEOTw4OwTANBgkqhkiG9w0BAQsFADBJMQswCQYDVQQG
EwJERTEZMBcGA1UEChMQUEtJLTEtVmVyd2FsdHVuZzEMMAoGA1UECxMDRE9JMREw
DwYDVQQDEwhET0kgQ0EgNTAeFw0xNTEyMDEwODMzMjJaFw0xODEyMDEyMzU5NTla
MIG9MQswCQYDVQQGEwJERTEdMBsGA1UEChMUTGFuZGVzdmVyd2FsdHVuZyBNLVYx
DTALBgNVBAsTBEVHVlAxGzAZBgNVBAsTElBvc3RmYWNoc2VydmVyIEdFUzERMA8G
A1UEBxMIU2Nod2VyaW4xIjAgBgkqhkiG9w0BCQEWE20uZGlua2F0dEBkdnotbXYu
ZGUxIDAeBgNVBAMTF0dSUDogUG9zdGZhY2hzZXJ2ZXItRFZaMQowCAYDVQQFEwEx
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAgIm3mQGpa/PtuChCN5b8
lWvzb+s6ETsUIjSgidwEC4VOx95Sy1D3AvOpJhJyUr2NUf0UVfFtOz/dJVmaqCME
Fp30rvpZz2RNASlJQZNVCKbaIA85ugsc4EzraM4n3pCZ0pKwfN7XJluQtd1oNVbW
I0TojspFoK8p1dhDFWec3h/3wBopmmpYmfKCUa/rqOYmIhWSOiBNi4Ef5GuhIEv1
c9DkZyCFUiKp8kg4pVnbfkyG4pZtajrERNZs5JnvAtSuwTAmg0GfqZ00vLXbS89m
EHS1NEiycez+KpeIkx9CDU+NCAxyz8rHj3IxDN1mz3KMjuJqT6gVQJOG3bEgLyQG
cQIDAQABo4ICIzCCAh8wcgYDVR0jBGswaYAUyeX4p3Uck+j6EceJE179huKM3XOh
SqRIMEYxCzAJBgNVBAYTAkRFMRkwFwYDVQQKExBQS0ktMS1WZXJ3YWx0dW5nMRww
GgYDVQQDExNQQ0EtMS1WZXJ3YWx0dW5nLTE0ggUAkLrc4TAeBgNVHREEFzAVgRNt
LmRpbmthdHRAZHZ6LW12LmRlMIIBIQYDVR0fBIIBGDCCARQwggEQoIIBDKCCAQiG
XGxkYXA6Ly94NTAwLmJ1bmQuZGUvQ049RE9JJTIwQ0ElMjA1LE9VPURPSSxPPVBL
SS0xLVZlcndhbHR1bmcsQz1ERT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0hmhs
ZGFwOi8vcGtpLWRpcmVjdG9yeS5kb2ktZGUubmV0L0NOPURPSSUyMENBJTIwNSxP
VT1ET0ksTz1QS0ktMS1WZXJ3YWx0dW5nLEM9REU/Y2VydGlmaWNhdGVSZXZvY2F0
aW9uTGlzdIY+aHR0cDovL3g1MDAuYnVuZC5kZS9jZ2ktYmluL3Nob3dfYXR0cj9j
bj1ET0klMjBDQSUyMDUmYXR0cj1jcmwwFgYDVR0gBA8wDTALBgkrBgEEAb10AQEw
DgYDVR0PAQH/BAQDAgXgMDwGCCsGAQUFBwEBBDAwLjAsBggrBgEFBQcwAYYgaHR0
cDovL29jc3AuZG9pLnRlbGVzZWMuZGUvb2NzcHIwDQYJKoZIhvcNAQELBQADggEB
AKvTBjZxIfDyo2oQNP4g4L+wcbME3wNJnszlpuPyPbOpdeU+CUrdZMLU/F769nPG
3RJxj0Vgzownx4TJUbR6KDFQU5SFzGhCGL5+wz6wb/RqiTDOwsGeV/FzmFBaKm96
82fsWBwoasLOYH5TNM6+wSsleMs4QAoMQFtl1b6xvPboLhHVF7uYXcgaO372vVRm
472uD3HsKfBV2Mz9PkBuNNK5BjxMZdp8Yt9/NPv85yjresmqwL0laQjt9OTZn3MK
NnkFzjIsO+tsg8CRCt3lvZ1yCA/k03vX36wJfgg1uOuTcTauy+L4OaKdb780o233
Ix5AF+STjegUViasWydNz2s=
-----END CERTIFICATE-----

Elektronische Signatur zur Prüfung der Integrität der Daten (Base64-Encoded)
============================================================
GosXMq2FTzf5+NQZ4wqO21G/zJfO3/9umkc7p2RXPoRoKW6YA8nDTG0kUdpz1wV7eVHXVcl+f3bW
+nR/vxq8okfOZi7oy5PqSBSH0pmV3F/pAcvmAjWjVpFHqvjorBmhX6prM7C5skrRfVy3zis7BjAo
XAh31NRH9+sX2jHFlMeaYmW0uUBuIHxUpa9McpcH+JKHPpcepAg66uYEZCl8PITqyuRXw6uZZRv9
uCdJnkw+fo4EfKTdNHotWHnpPcN6GN7J0NMYTOka20sEa8reenbnxXs9AqJE6YKhj86lFzVFx3l0
IHnkXJKMJfOcr5tf4ar9q0Y6Us4IVfB6Y7H/+g==
============================================================

...prüfen sie die Signatur gegen ihre Originaldatei.
Geeignete Informationen finden Sie hier:
https://www.openssl.org/docs/manmaster/apps/
Mit freundlichem Gruß ihr PFS-Team (DVZ)
```

4.2 Anhang 2: (spezifische Informationen zum Transportprotokoll OSCI)

Die bisher getroffenen Ausführungen sind allgemeiner Natur und betreffen alle zum Einsatz kommenden Transportprotokolle. Das Protokoll OSCI hat einige Spezifika, deren Kenntnis in Situationen der Fehleranalyse und -behebung wichtig ist. Die zur Anwendung kommende Versandkomponente für das Protokoll OSCI ist mit XTA gekennzeichnet und auf den Systemen der Teilnehmer für dieses Protokoll installiert. Nachfolgende Darstellungen geben Architektur und Ablauf beim Einsatz von OSCI an (Datenanlieferung an CBPay/Profiskal, Datenrücklauf zum Teilnehmer und Quittungserstellung).

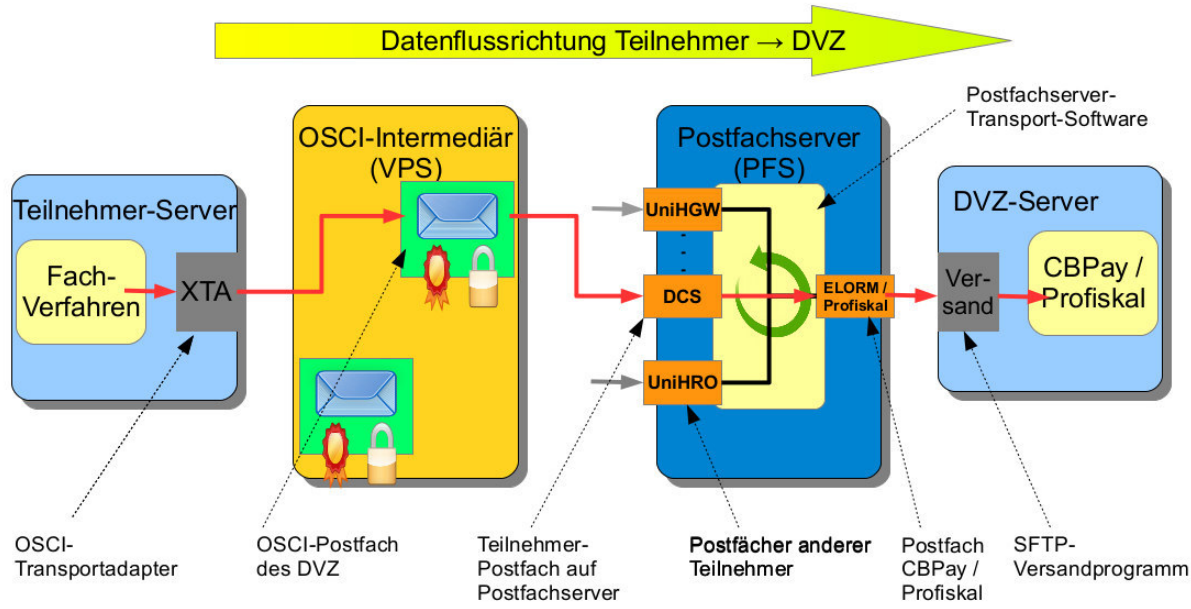

Abbildung 3: Datentransport externer Teilnehmer nach CBPay/Profiskal

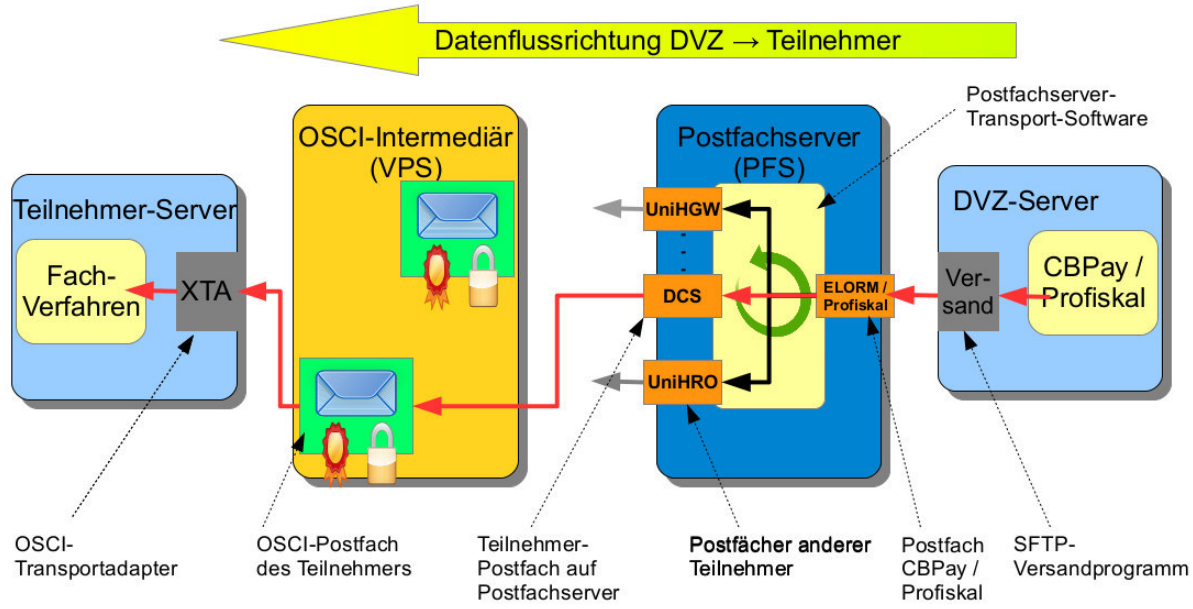

Abbildung 4: Datentransport CBPay/Profiskal zu externem Teilnehmer

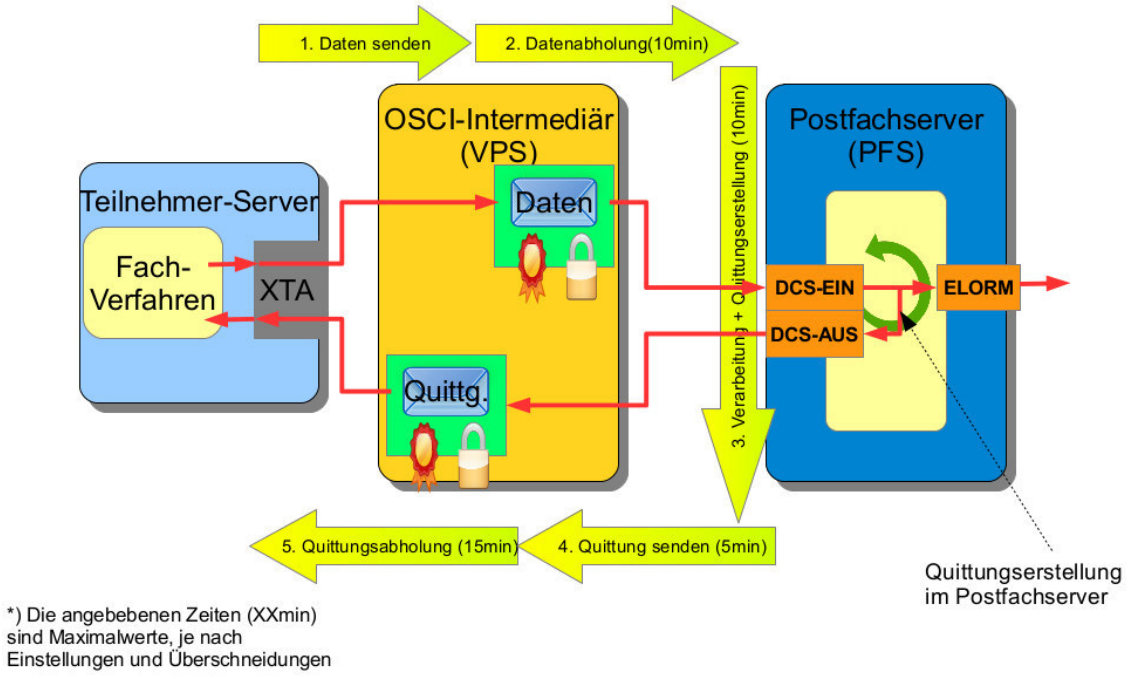

Abbildung 5: Ablauf der Quittungserstellung und zeitliche Reihenfolge

Bei Vorliegen eines Datentransferproblems, schicken Sie bitte dieses Formular ausgefüllt an unseren Service Desk: servicedesk@dvz-mv.de

Service

[x] ProFiskal

Ihre Kontaktdaten

Ansprechpartner: _____

Dienststelle: _____ Telefon: _____

E-Mail: _____

Zutreffendes bitte ankreuzen:

[ ] Fall a) Problem Datentransfer Verfahren → ProFiskal
[ ] Fall b) Problem Datentransfer ProFiskal → Verfahren

Bitte folgende Felder ausfüllen:

Dateiname: _____

Wenn Fall a) → Wann wurde die Batch-Input-Datei an ProFiskal verschickt

_____

Wenn Fall b) → Zu welcher Batch-Input-Datei (Angabe Dateiname oder Versendetag) fehlt die zugehörige SST-Datei (= Quittungsdatei)

_____

Wenn Fall b) → Wenn eine IBE-Datei (= Ist-Rückmeldungen) fehlt, von welchem Tag fehlen die Buchungen

_____

Auswirkung

[ ] 1 = großflächig/verbreitet
[ ] 2 = erheblich/groß
[ ] 3 = moderat/begrenzt (Standard)
[ ] 4 = gering/lokal

Dringlichkeit

[ ] 1 = kritisch [ ] 2 = hoch [ ] 3 = mittel (Standard) [ ] 4 = niedrig

Bei Vorliegen eines Datentransferproblems, schicken Sie bitte dieses Formular ausgefüllt an unseren Service Desk: servicedesk@dvz-mv.de

Service [x] CBPay

Ihre Kontaktdaten

Ansprechpartner: _____

Dienststelle: _____ Telefon: _____

E-Mail: _____

Zutreffendes bitte ankreuzen:

☐ Fall a) Problem Datentransfer Verfahren → CBPay
☐ Fall b) Problem Datentransfer CBPay → Verfahren

Bitte folgende Felder ausfüllen:

Dateiname: _____

Anzahl der Dateisätze: ☐

Höhe der Dateisumme: ☐

Tag & Uhrzeit der Dateiversendung: _____

Für DCS: Kto.-Nr.: ☐ 1507 ☐ 1509 ☐ 1515

lfd. Dateinummer: _____

Auswirkung

☐ 1 = großflächig/verbreitet ☐ 2 = erheblich/groß
☐ 3 = moderat/begrenzt (Standard) ☐ 4 = gering/lokal

Dringlichkeit

☐ 1 = kritisch ☐ 2 = hoch ☐ 3 = mittel (Standard) ☐ 4 = niedrig

Dienststelle

Finanzministerium
Mecklenburg-Vorpommern
Referat IV 170
Schloßstraße 9-11
19053 Schwerin

Antrag auf Einwilligung gemäß VV Nr. 6.6 zu §§ 70-80 LHO M-V

☐ **für die Einführung eines IT-Verfahrens**
☐ **für die Änderung eines IT-Verfahrens**

Bezeichnung des IT-Verfahrens

verantwortliche Oberste Landesbehörde (OLB)

verantwortliche Stelle gemäß Nr. 2 der Anlage 6 zu VV zu §§ 70-80 LHO M-V (falls abweichend)

Das IT-Verfahren verfügt über eine automatisierte Schnittstelle zu	
☐	ProFiskal
☐	CBPay

Betreiber des Verfahrens (Standort)

Hersteller des Verfahrens (falls von Betreiber abweichend)

Ansprechpartner		
fachlich	Name:	
	Telefon:	
	E-Mail:	
technisch	Name:	
	Telefon:	
	E-Mail:	

Folgende für die Einwilligung erforderliche Unterlagen sind dem Antrag beigefügt:

- ☐ Verfahrensdokumentation (VV Nr. 6.2 zu §§ 70-80 LHO M-V)
- ☐ Gefährdungsanalyse (VV Nr. 6.3 zu §§ 70-80 LHO M-V)
- ☐ Ordnungsmäßigkeitskonzept (VV Nr. 6.4 zu §§ 70-80 LHO M-V)
- ☐ Prüfliste zur Einhaltung der kassenrechtlichen Vorschriften gemäß VV zu §§ 70-80 LHO M-V und VerfRi-IT-HKR
- ☐ bei Änderung von IT-Verfahren: Beschreibung der Änderung und Analyse der mit der Änderung verbundenen Risiken

Zeitpunkt (vorbehaltliche Einwilligung des FM)	
☐	Die Entwicklung des o.g. IT-Verfahrens ist abgeschlossen. Der Einsatz ist vorgesehen ab:
☐	Das o.g. IT-Verfahren wird/wurde geändert. Der Einsatz ist vorgesehen ab:

Erklärung:

Ein Sicherheitskonzept gemäß IT-Grundschutz des Bundesamtes für Sicherheit und Informationstechnik liegt in aktueller Form vor und wird entsprechend umgesetzt.

Bei Einsatz des IT-Verfahrens wird die Einhaltung der Bestimmungen nach VV Nr. 6 VV zu §§ 70-80 LHO einschließlich Anlage 6 (GoBIT-HKR) und der Verfahrensrichtlinie zum Einsatz von IT-Verfahren im Haushalts-, Kassen- und Rechnungswesen im Land Mecklenburg-Vorpommern (VerfRi-IT-HKR) gewährleistet. Die aktuell gültigen datenschutzrechtlichen Bestimmungen werden beachtet und umgesetzt.

Für die Richtigkeit		
	Datum	**Unterschrift Beauftragter für den Haushalt (Nr. 2 VerfRi-IT-HKR), Name in Druckbuchstaben**

Dienststelle

Finanzministerium
Mecklenburg-Vorpommern
Referat IV 170
Schloßstraße 9-11
19053 Schwerin

Erhebungsbogen für IT-Verfahren im Haushalts-, Kassen- und Rechnungswesen

Bezeichnung des IT-Verfahrens

Kurzbeschreibung Inhalt

verantwortliche Oberste Landesbehörde (OLB)

anwendende Behörde(n)/ Dienststelle(n)

Datum der letzten Einwilligung:	

Wurden seit der letzten Einwilligung des FM Änderungen im Verfahren vorgenommen?

Sind aktuell Änderungen am IT-Verfahren vorgesehen?

Ab welchem Zeitpunkt soll das geänderten Verfahren planmäßig eingesetzt werden?

aktuell produktive Version (Bezeichnung, Stand)

Übermittlungsintervalle/-zeiten an	
ProFiskal	
CBPay	

Betreiber des Verfahrens (Standort)

Hersteller des Verfahrens (falls von Betreiber abweichend)

Ansprechpartner		
fachlich	Name:	
	Telefon:	
	E-Mail:	
technisch	Name:	
	Telefon:	
	E-Mail:	

sonstige Anmerkungen

Hiermit wird bestätigt, dass nach VV Nr. 6.2 bis 6.5 zu §§ 70-80 LHO erforderliche Unterlagen (Verfahrensdokumentation, Gefährdungsanalyse, Ordnungsmäßigkeitskonzept) in aktueller Version vorliegen und umgesetzt werden.

Hinweis:
Die beim Inkrafttreten der aktuellen VV zu §§ 70-80 LHO und der VerfRi-IT-HKR in Betrieb befindlichen genehmigten Verfahren müssen die sich hieraus ergebenden Vorgaben spätestens dann erfüllen, wenn eine maschinelle Schnittstelle zum HKR-Verfahren oder Zahlungsverkehrsverfahren des Landes eingerichtet oder das IT-Verfahren wesentlich geändert wird.

Ein Sicherheitskonzept gemäß IT-Grundschutz des Bundesamtes für Sicherheit und Informationstechnik liegt in aktueller Form vor und wird entsprechend umgesetzt.

Die Bestimmungen der VV Nr. 6 VV zu §§ 70-80 LHO einschließlich Anlage 6 (GoBIT-HKR) und der Verfahrensrichtlinie zum Einsatz von IT-Verfahren im Haushalts-, Kassen- und Rechnungswesen im Land Mecklenburg-Vorpommern (VerfRi-IT-HKR) sowie die aktuell gültigen datenschutzrechtlichen Bestimmungen werden beim Betrieb des IT-Verfahrens vollständig beachtet und umgesetzt.

Für die Richtigkeit		
	Datum	**Unterschrift Beauftragter für den Haushalt (Nr. 2 VerfRi-IT-HKR), Name in Druckbuchstaben**

Verfahrensdokumentation

gemäß VV Nr. 6.2 zu §§ 70-80 LHO M-V

für das IT-Verfahren

…

Verfasser: …
Erstellungsdatum: …

Vorbemerkung

Die Verfahrensdokumentation dient dazu, einen Überblick über das IT-Verfahren zu verschaffen. Sie erleichtert die Prüfung, ob die kassenrechtlichen Vorgaben erfüllt werden, welche in den Verwaltungsvorschriften für Zahlungen, Buchführung und Rechnungslegung (VV zu §§ 70-80 LHO M-V) und den dazugehörigen Anlagen sowie in der Verfahrensrichtlinie zum Einsatz von IT-Verfahren im Haushalts-, Kassen- und Rechnungswesen im Land Mecklenburg-Vorpommern (VerfRi-IT-HKR) niedergelegt sind. Diese Vorgaben richten sich partiell nach der Ausgestaltung des IT-Verfahrens. Beispielsweise müssen die Anforderungen an die Verwendung von Stichprobenkontrollverfahren nur dann erfüllt werden, wenn tatsächlich ein solches Verfahren verwendet wird. Allerdings sind auch viele Anforderungen unabhängig von der konkreten Ausgestaltung gleich.

Aufgrund dessen beschränkt sich das vorliegende Muster auf Vorgaben zur Gliederung und zu einzelnen Inhalten. Ergänzt werden diese um Hinweise. Bei Abweichungen von diesen Vorgaben ist zu berücksichtigen, dass dies in der Regel zu erhöhtem Prüfungsaufwand und somit zu einer längeren Bearbeitungszeit führt. Ihr Ansprechpartner im Finanzministerium ist das Referat IV 170 (Haushaltsvollzug).

Inhalt

1. Einführung

Inhaltliche Vorgaben:

Im Rahmen der Einführung sollen der Hintergrund des IT-Verfahrens, die damit verfolgten Ziele sowie wichtige Eckpunkte des IT-Verfahrens kurz dargelegt werden. Dabei sind folgende Punkte zu thematisieren:

- Welche Ziele werden mit dem IT-Verfahren verfolgt?
- Welche Sachverhalte werden mit dem IT-Verfahren bearbeitet?
- Beruht das IT-Verfahren auf bereits im Einsatz befindlichen IT-Verfahren oder wird durch das IT-Verfahren ein im Einsatz befindliches IT-Verfahren abgelöst? Liegen für das bereits im Einsatz befindliche Verfahren Zertifizierungen vor? Wenn ja, welche?
- Welchen Umfang, insbesondere in finanzieller Hinsicht, weist das IT-Verfahren auf?
- An wen oder von wem erfolgen Zahlungen?
- Ist der Anschluss an eine Schnittstelle vorgesehen?
- Zu welchem Zeitpunkt soll das IT-Verfahren erstmals eingesetzt werden?
- Entwickler
- Einführende Stelle
- Nutzer/Anwender (Angabe der Behörde)

2. Verantwortungsbereiche (Nr. 5.1 VerfRi-IT-HKR)

Inhaltliche Vorgaben:

Bei IT-Verfahren für das Haushalts-, Kassen- und Rechnungswesen sind nach den Vorgaben der Nr. 5.1.5 VerfRi-IT-HKR die Funktionen

- der Aufgabenerfüllung,
- der Verfahrensentwicklung und -pflege sowie
- der technischen Durchführung

organisatorisch und personell zu trennen. Diese Trennung ist in der Verfahrensdokumentation zu belegen.
Ausführungen zur Berechtigungsvergabe und Berechtigungsverwaltung (siehe Nr. 5.1.1 VerfRi-IT-HKR) sind im Ordnungsmäßigkeitskonzept (Berechtigungskonzept) vorzunehmen (siehe Muster-Ordnungsmäßigkeitskonzept).

3. Zugriff auf das IT-Verfahren (Nr. 5.6 VerfRi-IT-HKR)

Inhaltliche Vorgaben:

Bezüglich des Zugriffs auf das IT-Verfahren sind folgende Punkte darzulegen:

- Welche Personen und Personengruppen haben Zugriff auf das IT-Verfahren?
- Wie erfolgt der Zugriff auf das IT-Verfahren? Ist eine Passworteingabe erforderlich?
- Bedarf die Nutzung bestimmter Funktionen des IT-Verfahrens einer zusätzlichen Passworteingabe?
- Wie erfolgt die Passwortvergabe? Welche Anforderungen werden an die Ausgestaltung der Passwörter gestellt?
- Welche weiteren Sicherheitsmaßnahmen bestehen, um einen Zugriff von Nichtberechtigten auf das IT-Verfahren zu verhindern?

4. Datenerfassung und -verarbeitung (Nr. 5 VerfRi-IT-HKR)

Zur Gewährleistung der Kassensicherheit kommt der vollständigen und ordnungsgemäßen Datenerfassung und -verarbeitung besondere Bedeutung zu. Dies ist der Grund für die umfangreichen Vorgaben in Nr. 5 VerfRi-IT-HKR. Gleichzeitig bedarf es somit einer genauen Darstellung der Abläufe zur Datenerfassung und -verarbeitung. Die textlichen Erläuterungen sollten dabei nach Möglichkeit um grafische Darstellungen ergänzt werden.

Inhaltliche Vorgaben:

Es sind folgende Punkte zu thematisieren:

- Werden mit dem IT-Verfahren Stammdaten verwaltet?
- Wie und von wem werden die Daten ermittelt (Nr. 5.2 VerfRi-IT-HKR)?
- Werden Daten aus anderen IT-Verfahren Verfahren übernommen (Nr. 5.3.1 VerfRi-IT-HKR)? Wenn ja, von wem werden die Daten übernommen? Wie wird die Richtigkeit und Vollständigkeit der Daten geprüft?
- Erfolgen vor der Datenerfassung eine schriftliche Feststellung der sachlichen und rechnerischen Richtigkeit und eine schriftliche Anordnung (Anlage 2 zu §§ 70-80 LHO M-V)?
- Wie und von wem werden die Daten erfasst (Nr. 5.3 VerfRi-IT-HKR)? Welche Verantwortlichkeiten werden vom Datenerfasser übernommen (Nr. 5.3.2 und Nr. 5.3.3 VerfRi-IT-HKR)?
- Wie erfolgt die Bescheinigung der Richtigkeit und Vollständigkeit der Daten nach Nr. 5.3.2 VerfRi-IT-HKR?
- Werden die Daten vor der Freigabe nach Nr. 5.4 VerfRi-IT-HKR auf Richtigkeit und Vollständigkeit geprüft? Wenn nein, wie ist das Stichprobenkontrollverfahren ausgestaltet?
- Wie wird die Prüfung der Daten bescheinigt?
- Können die Daten bei der Prüfung verändert werden? Wie wird vorgegangen, wenn Fehler festgestellt werden?
- Wie und von wem erfolgt die Freigabe der Daten nach Nr. 5.5.1 VerfRi-IT-HKR?
- Wie wird sichergestellt, dass bereits verarbeitete Daten nicht erneut verarbeitet werden?
- Werden die freigegebenen Daten an andere Verfahren übergeben? Wie und in welchen zeitlichen Abständen erfolgt die Übergabe?
- Welche Kontrollen werden durchgeführt, dass die gesendeten Datensätze richtig empfangen werden? Welche Maßnahmen werden bei fehlerhaften Übertragungen ergriffen?
- Werden die an andere IT-Verfahren zu übertragenden Datensätze zusammen mit der jeweiligen User-ID oder System-ID übergeben? Wenn nein, wie wird sichergestellt, dass die Datensätze nach der Übertragung dem jeweiligen Verursacher zugeordnet werden können?

5. Revisionsfähigkeit des Verfahrens (Nr. 5.8 VerfRi-IT-HKR)

Durch die Revisionsfähigkeit des IT-Verfahrens wird es ermöglicht, die Erledigung von Aufgaben mit Bezug zum Haushalts-, Kassen- und Rechnungswesen nachträglich auf ihre Ordnungsmäßigkeit zu überprüfen. Dazu müssen sämtliche Geschäftsvorfälle dokumentiert werden. Die Dokumentation muss so archiviert werden, dass sie von Dritten ohne große Mühe nachvollzogen werden kann. Insbesondere müssen Buchungen über eine Schnittstelle hinaus sowohl retrograd als auch progressiv zurück verfolgbar sein.

Inhaltliche Vorgaben:

In der Verfahrensdokumentation sind folgende Fragen zu beantworten:

- Wie wird sichergestellt, dass sämtliche buchführungspflichtigen Geschäftsvorfälle von einem Dritten in angemessener Zeit auf formelle und materielle Richtigkeit prüfbar sind?
- Wie werden Zugriffe und Geschäftsvorfälle dokumentiert? Welche Informationen werden dabei erfasst? Wer hat Zugriff auf die Dokumentation?
- Wie wird gewährleistet, dass Nachweise nach ihrer Erstellung nicht mehr verändert werden können?
- Kann die Darstellung der Geschäftsvorfälle vollständig oder auszugsweise geordnet nach Zeitpunkt, Sach- und Personenkonten erfolgen?
- Sind im IT-Verfahren Berechtigungen (z. B. eine vordefinierte Prüferrolle) eingerichtet, die durch direkte Zuordnung zu einer Person einen lesenden Zugriff auf alle Daten und Systemeinstellungen des IT-Verfahrens ermöglichen?
- Sind die Geschäftsvorfälle sowohl retrograd als auch progressiv prüfbar und ist hierbei immer eine eindeutige Zuordnung gewährleistet?

Der Aufbau des IT-Verfahrens, durch den die Revisionsfähigkeit des Verfahrens gewährleistet wird, ist detailliert und nachprüfbar, gleichzeitig aber auch für Normalanwender von Computern verständlich zu erläutern.

6. IT-Sicherheit (Nr. 5.9 VerfRi-IT-HKR)

Inhaltliche Vorgaben:

IT-Verfahren dürfen nur eingesetzt werden, wenn hinreichende Vorkehrungen gegen den Verlust und die Manipulation gespeicherter Daten getroffen worden sind. Die Verfahrensdokumentation muss daher zu folgenden Punkten Auskunft geben:

- Liegt eine Freigabe für das IT-Verfahren vor (vgl. Nr. 5.9.3 VerfRi-IT-HKR)?
- Durch wen wird das IT-Verfahren betrieben?
- Welche Sicherheitsmaßnahmen sind nach Nr. 5.9.1 VerfRi-IT-HKR zum Schutz vor unberechtigten Zugriffen sowie zum Schutz des Datenbanksystems, der Schnittstellen und der Datenübertragungen getroffen worden?
- In welchen zeitlichen Abständen wird der Daten- und Programmbestand gesichert? Wo werden die Sicherheitskopien aufbewahrt?
- Wie ist organisatorisch sichergestellt, dass entstehende oder sichtbar werdende Programmfehler oder Sicherheitslücken nach Nr. 5.9.4 VerfRi-IT-HKR in angemessener Zeit beseitigt werden können?
- Liegt ein Sicherheitskonzept nach BSI vor?

Hinweise:

Die ergriffenen technischen Sicherheitsmaßnahmen sind detailliert und nachprüfbar, gleichzeitig aber auch für Normalanwender von Computern verständlich darzulegen. Beruhen die getroffenen Sicherheitsmaßnahmen auf Sicherheitskonzepten oder liegt für die Sicherheitsmaßnahmen eine Zertifizierung (z. B. vom Bundesamt für Sicherheit in der Informationstechnik (BSI)) vor, kann auf eine nähere Darstellung der Sicherheitsmaßnahmen verzichtet werden. Durch die gemäß Nr. 2 VerfRi-IT-HKR zuständige Stelle, i.d.R. der Beauftragte für den Haushalt (BfH), ist zu bestätigen, dass ein Sicherheitskonzept gemäß IT-Grundschutz des Bundesamtes für Sicherheit und Informationstechnik in aktueller Form vorliegt und umgesetzt wird.

Hinsichtlich der organisatorischen Vorkehrungen ist nicht nur zu erläutern, ob und wie gewährleistet ist, dass das IT-Verfahren nicht umprogrammiert werden kann. Es sind ferner die Verfahrensabläufe zu skizzieren, die im Fall des Auftretens von Programmfehlern oder Sicherheitslücken anzuwenden sind.

7. Interne Kontrollen zur Einhaltung des Kassenrechts (Nr. 5.10 VerfRi-IT-HKR)

Inhaltliche Vorgaben:

Auch während des Einsatzes des IT-Verfahrens ist die Einhaltung der kassenrechtlichen Vorschriften regelmäßig zu überprüfen. In der Verfahrensdokumentation sind daher Ausführungen zu folgenden Punkten notwendig:

- Welche Kontrollen sind vorgesehen, um während des Einsatzes des IT-Verfahrens die Einhaltung der kassenrechtlichen Vorschriften sicherzustellen? (Bitte die maschinellen und manuellen Kontrollen getrennt erläutern.)
- Wird im Rahmen der Kontrollen überprüft, ob das eingesetzte IT-Verfahren dem dokumentierten und genehmigten Verfahren entspricht?
- In welchen Zeiträumen finden die Kontrollen statt?
- Wer ist für die Durchführung der Kontrollen verantwortlich?
- Wie werden die Kontrollen dokumentiert?

8. Archivierung aufbewahrungspflichtiger Unterlagen

Die Archivierung der Belege ist gemäß VV Nr. 4.7 sowie Nr. 6 der Anlage 6 zu §§ 70-80 LHO M-V darzustellen.

Inhaltliche Vorgaben:

Erforderlich sind Angaben zu folgenden Punkten:

- Erfolgt die Archivierung papiergestützt oder elektronisch?
- Werden schriftliche Unterlagen in eine elektronische Form übertragen?
- Welche Unterlagen werden aufbewahrt?
- An welchem Ort und in welcher Weise werden die Unterlagen aufbewahrt?
- Wie wird gewährleistet, dass Anordnungen den begründenden Unterlagen zugeordnet werden können?
- Für welche Zeiträume werden die Unterlagen archiviert?

Gefährdungsanalyse

gemäß VV Nr. 6.3 zu §§ 70-80 LHO M-V

für das IT-Verfahren

…

Verfasser: …
Erstellungsdatum: …

Vorbemerkung

Das vorliegende Muster ist als Hilfestellung für die Erstellung einer kassenrechtlichen Gefährdungsanalyse i. S. v. VV Nr. 6.3 zu §§ 70-80 LHO M-V konzipiert.
Die Nutzung des IT-Verfahrens darf die Kassensicherheit nicht gefährden (Nr. 1.3 Verfahrensrichtlinie zum Einsatz von IT-Verfahren im Haushalts-, Kassen- und Rechnungswesen im Land Mecklenburg-Vorpommern (VerfRi-IT-HKR)). Dementsprechend sind sowohl die Einführung als auch die Änderung eines IT-Verfahrens nur zulässig, soweit Risiken für die Kassensicherheit durch technische oder organisatorische Maßnahmen wirksam beherrscht werden können. Eine Gefährdungsanalyse ist für jedes IT-Verfahren zu erstellen, unabhängig davon, ob es kassenrechtliche Ausnahmen, z.B. Abweichungen zum Vier-Augen-Prinzip beansprucht oder nicht. Nähere Anforderungen an die Gefährdungsanalyse legt Nr. 7.4.2 VerfRi-IT-HKR fest. Dabei ist zu berücksichtigen, dass eine Gefährdung der Kassensicherheit nicht nur bei Betrachtung eines jeweiligen Einzelrisikos vorliegen kann, sondern sich auch aus der kumulierten Betrachtung mehrerer Einzelrisiken ergeben kann.

Das vorliegende Muster für eine Gefährdungsanalyse enthält Vorgaben zur Gliederung und zu Inhalten, die bei einzelnen Gliederungspunkten behandelt werden sollten. Bei Abweichungen von diesen Vorgaben ist zu berücksichtigen, dass dies in der Regel zu erhöhtem Prüfungsaufwand und somit zu einer längeren Bearbeitungszeit seitens der einwilligenden Stelle führt. Für Rückfragen ist das Referat IV 170 (Haushaltsvollzug) Ihr Ansprechpartner.

Inhalt

1. Risikoidentifikation und Risikocharakterisierung

Inhaltliche Vorgaben:

Zunächst sind sämtliche Risiken, die durch die Nutzung des IT-Verfahrens für die Kassensicherheit entstehen können, zu identifizieren. In erster Linie sind hiermit Missbrauchsmöglichkeiten durch die Anwender des IT-Verfahrens oder durch Außenstehende gemeint. Hierzu gehören aber auch möglicherweise auftretende technische Fehler des IT-Verfahrens (IT-Sicherheit), Risiken für die Revisionssicherheit (z.B. im Zusammenhang mit Fehlern bei Datenübernahmen oder Datentransporten) etc., da dadurch die Kassensicherheit des IT-Verfahrens ebenfalls gefährdet sein kann. Je nachdem wie komplex das IT-Verfahren ist, empfiehlt sich sowohl eine gesonderte Betrachtung einzelner Prozesse innerhalb des Verfahrens als auch eine Gesamtbetrachtung des IT-Verfahrens hinsichtlich möglicher Risiken.

z. B.: Risiko des Zugriffs durch Unbefugte auf das IT-Verfahren, Manipulation von zahlungsrelevanten Daten durch Administratoren, Datenverlust beim Transport der Daten, Manipulation von zahlungsrelevanten Daten bei der Umwandlung von (papiernen) Originalbelegen in elektronische Belege etc.

Risiken ergeben sich zudem fast immer, wenn von den kassenrechtlichen Vorschriften abgewichen wird.

z. B.: Risiko infolge des Einsatzes eines Stichprobenkontrollverfahrens anstelle des Vier-Augen-Prinzips, Risiko bei Verzicht auf die Bescheinigung der ordnungsgemäßen und vollständigen Datenerfassung bei Stammdatenerfassung etc.

Art, Ursprung und Folgen des jeweiligen Risikos sind so zu beschreiben, dass dies von Dritten nachvollzogen werden kann. Im Falle einer Abweichung von einer kassenrechtlichen Vorschrift ist dies zu begründen.

z. B.: Beim IT-Verfahren <Name IT-Verfahren> erfolgt die Datenerfassung im System lediglich durch eine einzelne Person. Eine regelmäßige Kontrolle der ordnungsgemäßen und vollständigen Datenerfassung durch eine zweite Person ist nicht vorgesehen. Die Datenprüfung wird lediglich stichprobenartig durch eine zweite Person, hier den Vorgesetzten, durchgeführt. Es besteht somit das Risiko, dass Fehler bei der Datenerfassung nicht in jedem Fall erkannt werden und somit eine falsche Zahlung angeordnet wird.
Durch die Abweichung von VV Nr. 1.1.2 zu §§ 70-80 LHO M-V (Nr. 5.1.4 VerfRi-IT-HKR) und damit durch den Verzicht auf eine durchgängige Vier-Augen-Prüfung können Einsparungen hinsichtlich … erbracht werden.

2. Risikoquantifizierung und Risikobewertung

Inhaltliche Vorgaben:

Im zweiten Schritt der Gefährdungsanalyse sind die Risiken zu quantifizieren und zu bewerten. Wie groß das Risiko tatsächlich ist, ergibt sich aus dem Zusammenwirken von seiner Eintrittswahrscheinlichkeit und dem Ausmaß der negativen Folgen (Schadensausmaß).

Risikoquantifizierung

Vor Schätzung der Eintrittswahrscheinlichkeit und des Schadensausmaßes sind zunächst die ergriffenen Sicherheitsvorkehrungen/Schutzmaßnahmen zur Risikoprävention bzw. Risikominderung zu beschreiben. Hier sollten sämtliche technischen oder organisatorischen Maßnahmen zur Verringerung der Eintrittswahrscheinlichkeit oder zur Minderung des Schadensausmaßes bezüglich des Risikos geschildert werden.

z. B.: systemtechnische Plausibilitätskontrollen oder systemtechnische Vorgaben zur Vermeidung von Eingabefehlern bei der Datenerfassung, regelmäßige Rücklaufkontrollen um Fehler oder Missbrauch aufzudecken, Saldenabgleich o.ä. systemtechnische Kontrollen zur Sicherstellung des ordnungsgemäßen Datentransports, nachträgliche stichprobenhafte Kontrolle von Abrechnungen der Vertragspartner etc.

Unter Berücksichtigung der ergriffenen Schutzmaßnahmen ist die verbleibende Eintrittswahrscheinlichkeit des Risikos schätzen.

Bei der Schätzung sind, sofern möglich, Erfahrungen aus ähnlichen IT-Verfahren oder Altverfahren zu berücksichtigen. Handelt es sich um ein völlig neues IT-Verfahren, so ist die Schätzung der Eintrittswahrscheinlichkeit eine erste Einschätzung, die gegebenenfalls nach einer gewissen Zeit der Inbetriebnahme des Verfahrens korrigiert werden muss. Die Schätzung ist zu begründen.

Risikobewertung

Das ermittelte Risiko für die Kassensicherheit muss beherrschbar sein. Ein Risiko gilt als nicht mehr beherrschbar, wenn dessen Eintrittswahrscheinlichkeit in Bezug auf die Gesamtzahl der Geschäftsvorfälle hoch ist (Eintrittswahrscheinlichkeit 10 bis 100 Prozent).
Sofern ein Risiko nicht als unbeherrschbar gilt, ist im Rahmen der Risikobewertung darzulegen, warum es akzeptabel ist und warum auf das Ergreifen weiterer Schutzmaßnahmen verzichtet wird.

z. B.: Kosten-Nutzen-Analyse => Abwägung des Nutzens einer Risikoreduzierung mit dem dafür benötigten Aufwand, Vergleich mit anderen tolerierten Risiken => Ist das Risiko geringer als bereits akzeptierte Risiken?

Prüfungsschema

Für die Risikocharakterisierung, -quantifizierung und –bewertung empfiehlt sich folgende Darstellung:

I. Beschreibung des Risikos	Das Risiko ist detailliert zu beschreiben. Im Falle einer Abweichung von einer kassenrechtlichen Vorschrift ist diese zu benennen. Des Weiteren sind die Folgen für die Kassensicherheit bei Eintritt des Risikos zu erläutern. Die Beschreibung muss von externen Dritten nachvollzogen werden können.
II. Ergriffene Schutzmaßnahmen	Es sind die ergriffenen Schutzmaßnahmen zur Reduzierung des unter 1. beschriebenen Risikos zu erläutern. Dazu gehören insbesondere technische und organisatorische Gegenmaßnahmen sowie die Einrichtung eines Fehlermanagements.

III. Bewertung des nach Einführung der Schutzmaßnahmen verbleibenden Risikos				
a) Eintrittswahrscheinlichkeit in Bezug auf die Gesamtzahl der Geschäftsvorfälle	0 - 0,1 Prozent	0,1 – 2,5 Prozent	2,5 – 10 Prozent	10 – 100 Prozent
	Das Risiko ist infolge der ergriffenen Schutzmaßnahmen sicher ausgeschlossen.	Die Wahrscheinlichkeit des Risikoeintritts ist verschwindend gering.	Es besteht eine signifikante Wahrscheinlichkeit, dass das Risiko eintreten wird.	Die Wahrscheinlichkeit des Risikoeintritts ist so hoch, dass der Eintritt nicht überraschend wäre.
b) Begründung	Die Risikoeinschätzung ist zu begründen. Dabei können insbesondere das aus früheren Verfahren gewonnene Erfahrungswissen und die ergriffenen Schutzmaßnahmen herangezogen werden.			
c) maximaler Schaden bei Risikoeintritt	Zu schätzen ist der bei Risikoeintritt maximal mögliche Schaden pro Fall/Jahr.			
d) Begründung und Bewertung	Es sind die Grundlagen zu erläutern, auf denen die Risikoeinschätzung beruht. Insbesondere folgende Aspekte können dabei berücksichtigt werden: maximaler finanzieller Umfang eines Geschäftsvorfalls, Gesamtanzahl der Geschäftsvorfälle und maximaler prozentualer Anteil der unrichtigen Geschäftsvorfälle. Das verbleibende Risiko ist nach Prüfung der Ausschlusskriterien zu bewerten. Hierbei ist auch zu begründen, warum von weiteren Schutzmaßnahmen zur Risikominimierung abgesehen wird.			

3. Risikokontrolle: Verfahren zur Überprüfung der Gefährdungsanalyse

Inhaltliche Vorgaben:

Die für das IT-Verfahren verantwortliche Stelle ist gemäß Nr. 10.1 VerfRi-IT-HKR verpflichtet, nach Einführung des IT-Verfahrens zu prüfen, ob auf Grundlage des gesammelten Erfahrungswissens die ursprüngliche Gefahreinschätzung weiterhin zutreffend ist. Die Prüfung ist zu dokumentieren.

In der Gefährdungsanalyse sind hierzu folgende Angaben zu machen:

I. Verantwortliche Person	Es ist eine Person zu benennen, die für die Durchführung der Risikokontrolle verantwortlich ist.

II. Ausgestaltung der Risikokontrolle	Die Nr. 10.1 VerfRi-IT-HKR enthält keine verbindlichen Vorgaben, wie die Risikokontrolle auszugestalten ist. Diesbezüglich sind eine Vielzahl von Verfahren möglich, beispielsweise eine schriftliche Befragung der Anwender mittels Fragebögen, eine statistische Auswertung oder eine Evaluation durch Externe. Welches Verfahren am besten geeignet ist, ist von den Spezifika des jeweiligen IT-Verfahrens abhängig. Der für das IT-Verfahren zuständigen Behörde steht aus diesem Grund ein Einschätzungsspielraum zu. Die Ausgestaltung ist entsprechend darzustellen.
III. Frequenz der Risikokontrolle	Es ist darzulegen, in welchen zeitlichen Abständen eine Überprüfung der Gefährdungsanalyse vorgesehen ist. Die Zeiträume zwischen den Überprüfungen dürfen nicht zu lang sein, um zu verhindern, dass die Schutzmaßnahmen auf einer unzureichenden Gefährdungsanalyse aufbauen.

Ordnungsmäßigkeitskonzept

gemäß VV Nr. 6.4. zu §§ 70-80 LHO

für das IT-Verfahren

…

Verfasser: …
Erstellungsdatum: …

Vorbemerkung

Funktion des Ordnungsmäßigkeitskonzeptes ist es, Einzelheiten zur Abgrenzung der Verantwortlichkeiten (Berechtigungsverwaltung des IT-Verfahrens -von der Einrichtung bis hin zur Löschung von Berechtigungen-) und die weiteren Maßnahmen zu beschreiben. Ziel einer ordnungsgemäßen Berechtigungsverwaltung ist, dass auf das IT-Verfahren lediglich Personen Zugriff haben, die den Zugriff für die Erledigung der ihnen übertragenen Dienstaufgabe benötigen und denen der Zugriff ordnungsgemäß übertragen worden ist. Darüber hinaus muss aus Gründen der Revisionssicherheit auch im Nachhinein nachvollziehbar sein, wer wann welche Berechtigung für das IT-Verfahren innehatte. Das vorliegende Muster für ein Ordnungsmäßigkeitskonzept enthält Vorgaben zur Gliederung und zu Inhalten, die bei einzelnen Gliederungspunkten behandelt werden sollten. Ergänzt werden diese Vorgaben um Beispiele.

Inhalt

1. Berechtigungsverwaltung

1.1 Benutzerrollen

Inhaltliche Vorgaben:

Eine Benutzerrolle fasst eine Menge von Einzel-Rechten des IT-Verfahrens zusammen. Dabei wird diese dazu verwendet, um die Einzel-Rechte der bestimmten Bereiche nicht für jeden Nutzer einzeln festlegen zu müssen. Die Benutzerrolle enthält die zuzuweisenden Rechte.
Die in einem IT-Verfahren vorhandenen Benutzerrollen sind Ausgangsbasis für die Vergabe von Berechtigungen. Sicherheitsmängel an dieser Stelle haben deshalb negative Auswirkungen auf das gesamte weitere IT-Verfahren. Zu dem Themenbereich Benutzerrollen muss das Ordnungsmäßigkeitskonzept aus diesem Grund folgende Angaben enthalten:

- Wer ist für die Einrichtung der Benutzerrollen zuständig?
- Welche Benutzerrollen sind für das IT-Verfahren eingerichtet worden?
- Können bei der Berechtigungsvergabe mehrere Benutzerrollen gleichzeitig herangezogen werden? Welche Kombinationsmöglichkeiten gibt es?
- Wie ist die Trennung von Anordnung, Buchung und Zahlung gewährleistet? Wie ist sichergestellt, dass nicht nur eine Person allein an einer Anordnung beteiligt ist?
- Sind Abweichungen von den Benutzerrollen bei der Berechtigungsvergabe zulässig? Wenn ja, unter welchen Voraussetzungen?
- Wer ist für die Pflege und Änderung der Benutzerrollen zuständig?
- Unter welchen Voraussetzungen und in welchem Verfahren dürfen Benutzerrollen geändert werden?

Ist abweichend von der Definition von Benutzerrollen im IT-Verfahren eine direkte Rechtevergabe vorgesehen, so ist diese entsprechend zu erläutern.

z. B.: Die Einrichtung der Benutzerrollen für das IT-Verfahren <Name IT-Verfahren> ist Aufgabe der <fachlich zuständige Stelle>. Diese hat folgende Benutzerrollen eingerichtet:

Name	
Technischer Name	
Art der Rolle	
Verwendung der Rolle	
Rollenbeschreibung:	
Mögliche Mitarbeitergruppen:	

[…] Bei der Berechtigungsvergabe können mehrere Benutzerrollen herangezogen werden, soweit dies in den vorherigen Beschreibungen nicht ausgeschlossen ist. […] Die Befugnisse, welche notwendig sind, um eine Zahlung anzuordnen, sind getrennt auf zwei Benutzerrollen (Feststellung, Anordnung) verteilt. Eine Anordnung kann infolgedessen ausschließlich dann erfolgen, wenn die Befugnisse aus beiden Benutzerrollen wahrgenommen werden. Dies setzt die Mitwirkung von zwei unterschiedlichen Personen voraus, da die Benutzerrollen „Feststellung“ und „Anordnung“ nicht gemeinsam bei der Rollenvergabe herangezogen werden dürfen. Das ist in den Rollenbeschreibungen ausdrücklich festgeschrieben. […] Abweichungen von den Vorgaben der Benutzerrollen bei der Berechtigungsvergabe sind nicht zulässig. […] Die Pflege und Änderung der Benutzerrollen obliegen ebenfalls der <fachlich zuständigen Stelle>.

Änderungen erfolgen nur, wenn eine ordnungsgemäße Aufgabenerledigung mit den vorhandenen Musterrollen nicht möglich ist. Des Weiteren bedürfen Änderungen eines schriftlichen Antrags des Beauftragten für den Haushalt. Änderungen der Benutzerrollen werden schriftlich dokumentiert. […]

1.2 Vergabe von Berechtigungen

Inhaltliche Vorgaben:

Für die Sicherheit der Berechtigungsvergabe ist entscheidend, dass für die Vergabe ein schriftliches Verfahren existiert. Dafür bedarf es zu den nachfolgenden Punkten einer Verfahrensregelung:

- Wer beantragt in welcher Form die Vergabe von Berechtigungen an Bedienstete?
- Wer entscheidet in welcher Form über die Vergabe von Berechtigungen?
- Welche Voraussetzungen müssen für die Vergabe erfüllt sein?
- Wer erzeugt in welchen Systemen die Berechtigungen?
- Welche Voraussetzungen müssen für die Erzeugung erfüllt sein?

z. B.: Neue Rollen und Anwender werden beim <Benennung Verantwortlicher> schriftlich beantragt. Im Antrag ist kurz darzulegen, welche Aufgaben die Anwender wahrnehmen sollen und welche Berechtigungen dafür erforderlich sind.

1.3 Änderung von Berechtigungen

Inhaltliche Vorgaben:

Im Kassenrecht gilt das Prinzip der minimalen Berechtigung. Dazu muss insbesondere gewährleistet sein, dass Bedienstete Berechtigungen nicht behalten, wenn sie diese für die Erledigung einer übertragenen Aufgabe nicht mehr benötigen. Solche Veränderungen treten insbesondere bei Arbeitsplatzwechseln auf. Die nachträgliche Erweiterung von Berechtigungen muss ebenfalls mit dem Prinzip der minimalen Berechtigung vereinbar sein. Daher bedarf es im Ordnungsmäßigkeitskonzept Regelungen zu folgenden Punkten:

- Unter welchen Voraussetzungen ist eine Änderung der Berechtigungen zwingend vorzunehmen?
- Welches Verfahren gilt bei der Änderung von Berechtigungen?
- Wie wird sichergestellt, dass Bediensteten Berechtigungen entzogen werden, wenn sie diese zur Erledigung der ihnen zugewiesenen Aufgaben nicht mehr benötigen?
- Welches Verfahren gilt beim Entzug von Berechtigungen?

z. B.: Bei der Veränderung von Aufgabenzuständigkeiten eines Anwenders prüft dessen Vorgesetzter, ob Änderungen bei der Berechtigungsvergabe erforderlich sind. […] Verlässt ein Anwender die Behörde oder wechselt er auf einen Arbeitsplatz, an dem er nicht mit Aufgaben im Zusammenhang mit <Name IT-Verfahren> betraut ist, wird dessen Berechtigung entzogen. Offene Aufgaben und Fälle sind einem zulässigen Benutzer zuzuordnen. Der Anwender ist durch die <verantwortliche Stelle> zu deaktivieren.

1.4 Nachweis der Verwaltung von Berechtigungen

Inhaltliche Vorgaben:

Die Revisionsfähigkeit eines IT-Verfahrens setzt voraus, dass die Verwaltung der Berechtigungen nachvollzogen werden kann. Zu den nachstehenden Punkten sind aus diesem Grund Regelungen zu treffen:

- Wie wird die Verwaltung von Berechtigungen (Einrichtung, Erweiterung, Veränderung, Entzug und Löschung) dokumentiert?
- Wie wird die Identität der an der Zuweisung beteiligten Personen nachgewiesen?
- Für welchen Zeitraum wird die Dokumentation archiviert?

z. B.: Die Neuanlage oder Änderung von Rollen wird schriftlich dokumentiert. Dazu werden die mit der Dokumentationsfunktion der elektronischen Benutzerverwaltung von <Name IT-Verfahren> erfassten Daten (Name des Bearbeiters des Vorgangs, Art der Berechtigung, Name des Anwenders) zur Neuanlage oder Änderung ausgedruckt. Die ausgedruckten Formulare werden für die Dauer der Aufbewahrungsfrist durch die Behörde aufbewahrt.

1.5 Kontrolle der Einhaltung des Ordnungsmäßigkeitskonzepts

Inhaltliche Vorgaben:

Die durch die vorausgehenden Regelungen in der Theorie geschaffene Sicherheit vor unberechtigten Zugriffen tritt in der Praxis nur dann ein, wenn die Regelungen tatsächlich befolgt werden. Um dies zu gewährleisten, müssen u.a. Kontrollen durchgeführt werden. Wesentliche Eckpunkte solcher Kontrollen sind:

- In welcher Weise wird kontrolliert, dass die an der Verwaltung der Berechtigungen beteiligten Personen ihre Aufgaben ordnungsgemäß erfüllen?
- Wer ist für die Kontrolle zuständig? Wie wird die Kontrolle dokumentiert?
- Welches Verfahren ist bei Fehlern in der Berechtigungsvergabe vorgesehen?
- Welche Prüferrollen sind eingerichtet worden (genaue Darlegung der damit verbundenen Berechtigungen)?

z. B.: Der zuständige Beauftragte für den Haushalt oder eine von ihm bestimmte Person prüft stichprobenweise, ob die Vergabe von Berechtigungen inhaltlich richtig erfolgt und ordnungsgemäß dokumentiert worden ist. […]
Bestehen Anhaltspunkte, dass bei der Vergabe von Berechtigungen Fehler aufgetreten sind, ist die Berechtigungsvergabe unverzüglich zu stornieren. Die verantwortliche Stelle ist über die Anhaltspunkte schriftlich zu informieren. […] Die verantwortliche Stelle prüft, ob eine Stornierung der Berechtigung erforderlich ist oder der Fehler auf andere Weise beseitigt werden kann. Das Ergebnis der Prüfung muss schriftlich dokumentiert werden. […]

2. Weitere Maßnahmen gemäß VV Nr. 6.4.1 bis 6.4.6 zu §§ 70-80 LHO M-V

Der Ablauf des Anordnungsverfahrens ist unter dem Aspekt der Wahrnehmung der jeweiligen Verantwortlichkeiten zu beschreiben. Darüber hinaus sind die im IT-Verfahren implementierten Kontrollen und Prüfmechanismen darzulegen. Sind die Abläufe bereits in der Verfahrensdokumentation beschrieben, ist auf die entsprechenden Fundstellen zu verweisen.

z. B.: Nachdem die erforderlichen Daten durch den zuständigen Sachbearbeiter anhand der begründenden Unterlagen bzw. sonstigen Buchungsbelege erfasst wurden, veranlasst dieser die Ausführung der Berechnungsroutine. Das IT-Verfahren <Name IT-Verfahren> errechnet anhand vorprogrammierter Berechnungsalgorithmen die jeweiligen Leistungen. Der zuständige Sachbearbeiter gibt die Daten zur weiteren Bearbeitung frei (Feststellung der sachlichen und rechnerischen Richtigkeit).
Durch den zuständigen Prüfer <Benennung Verantwortlicher> werden die zahlungsrelevanten Daten geprüft und bei Feststellung der Richtigkeit zur weiteren Verarbeitung freigegeben (Wahrnehmung der Anordnungsbefugnis).
Durch den <Benennung Verantwortlicher> werden darüber hinaus Stichprobenkontrollen (mindestens 5% aller Zahlfälle) durchgeführt.

Prüfliste

zur Einhaltung der kassenrechtlichen Vorschriften

gemäß VV zu §§ 70-80 LHO M-V und VerfRi-IT-HKR ...

für das IT-Verfahren

...

Verfasser: …

Erstellungsdatum: …

Vorbemerkung

Die nachfolgende Prüfliste soll der für das IT-Verfahren verantwortlichen Stelle einen Überblick zu den wesentlichen kassenrechtlichen Vorschriften bieten, die von IT-Verfahren für das Haushalts-, Kassen- und Rechnungswesen einzuhalten sind. Gleichzeitig soll sie die Prüfung im Rahmen des Einwilligungsverfahrens gemäß VV Nr. 6.6 zu §§ 70-80 LHO M-V beschleunigen und erleichtern. Vor allem aber ist die Prüfliste eine Erklärung der für das IT-Verfahren verantwortlichen Stelle darüber, ob und inwieweit die kassenrechtlichen Vorschriften eingehalten werden. Die Prüfliste ist daher dem Antrag auf Einwilligung für das IT-Verfahren beizufügen.

Inhalt

I. Ansprechpartner

Verantwortliche Stelle nach Nr. 2 VerfRi-IT-HKR	• Bezeichnung und Anschrift der verantwortlichen Stelle • Name, Telefon und E-Mail-Adresse des Beauftragten für den Haushalt in der verantwortlichen Stelle • Name, Telefon und E-Mail-Adresse des Ansprechpartners für das Einwilligungsverfahren in der verantwortlichen Stelle
Hersteller/Betreiber des IT-Verfahrens	• Bezeichnung und Anschrift des Herstellers/Betreibers • Name, Telefon und E-Mail-Adresse des Ansprechpartners beim Hersteller/Betreiber
Fachlicher Ansprechpartner	• Bezeichnung und Anschrift des/der fachlichen Ansprechpartner(s) • Name, Telefon und E-Mail-Adresse des/der fachlichen Ansprechpartner(s)

II. Prüfliste zur Einhaltung der kassenrechtlichen Vorschriften

Hinweis: Die nachfolgende Liste ermöglicht es, selbstständig zu prüfen, ob ein IT-Verfahren die kassenrechtlichen Vorschriften einhält. Mit Ausnahme der blau unterlegten Felder sind die Fragen so konzipiert, dass bei einer Verneinung der Frage von kassenrechtlichen Vorschriften abgewichen wird.

1. Formelle Anforderungen (Nr. 7 der VerfRi-IT-HKR)

Existiert für das IT-Verfahren	
• eine Verfahrensdokumentation?	Ja/Nein
• eine Gefährdungsanalyse?	Ja/Nein
• ein Ordnungsmäßigkeitskonzept?	Ja/Nein
• eine Dienstanweisung?	Ja/Nein

2. Ordnungsmäßigkeitskonzept (Berechtigungskonzept nach VV Nr. 6.4 zu §§ 70-80 LHO M-V und Nr. 5.1 VerfRi-IT-HKR)

Enthält das Ordnungsmäßigkeitskonzept		
• eine Übersicht der eingerichteten Benutzerrollen?	Ja/Nein	*Fundstelle*
• Vorgaben, durch die die Trennung der Berechtigungen für Anordnung und Zahlung gewährleistet ist?	Ja/Nein	*Fundstelle*
• Vorgaben, durch die technisch sichergestellt ist, dass eine Person eine Anordnung nicht allein durchführen kann?	Ja/Nein	*Fundstelle*
• ein Verfahren für die Pflege, Änderung und Neueinrichtung von Benutzerrollen einschließlich der Dokumentation dieser Vorgänge?	Ja/Nein	*Fundstelle*
• ein Verfahren für die Vergabe von Berechtigungen?	Ja/Nein	*Fundstelle*
• ein Verfahren für die Änderung von Berechtigungen?	Ja/Nein	*Fundstelle*
• Regelungen zum Nachweis der Verwaltung von Berechtigungen?	Ja/Nein	*Fundstelle*
• Vorgaben zur Kontrolle der Einhaltung des Ordnungsmäßigkeitskonzepts?	Ja/Nein	*Fundstelle*
Ist sichergestellt, dass das IT-Verfahren nicht unbefugt ergänzt, verändert oder gelöscht werden kann?	Ja/Nein	*Fundstelle*
Sind die Funktionen der Aufgabenerfüllung von der Verfahrensentwicklung und -pflege getrennt?	Ja/Nein	*Fundstelle*
Stellt das Berechtigungsverwaltungsverfahren sicher, dass zu jedem Zeitpunkt festgestellt werden kann, welche Personen, einschließlich Administratoren und andere Systemverwalter, zu welchem Zeitpunkt mit welchen Berechtigungen ausgestattet gewesen sind?	Ja/Nein	*Fundstelle*

3. Zugriffskontrolle (Nr. 3.4 der Anlage 6 VV zu §§ 70-80 LHO M-V)

Ist das IT-Verfahren durch eine Zugriffskontrolle vor dem Zugriff Unbefugter geschützt?	Ja/Nein	*Fundstelle*
Bedarf es für den Zugriff auf das Verfahren der Eingabe eines Passwortes?	Ja/Nein	*Fundstelle*
Gibt es Vorgaben zur Ausgestaltung des Passwortes?	Ja/Nein	*Fundstelle*
Erfolgt der Zugriff auf das IT-Verfahren mittels Single-Sign-On?	Ja/Nein	*Fundstelle*

4. Richtigkeit der Datenermittlung, -erfassung und -verarbeitung

a) Datenerfassung durch manuelle oder andere Eingabe von Daten schriftlicher Unterlagen

Erfolgt eine Datenerfassung durch manuelle oder andere Eingabe von Daten schriftlicher Unterlagen?	Ja/Nein	*Fundstelle*
Hinweis: *Die nachfolgenden Fragen sind nur zu beantworten, wenn die vorherige Frage mit „Ja“ beantwortet wird.*		
Wird die vollständige und ordnungsgemäße Datenerfassung durch einen Sachbearbeiter bescheinigt?	Ja/Nein	*Fundstelle*
Erfolgt die Bescheinigung nach den Vorgaben der Nr. 5.3 VerfRi-IT-HKR?	Ja/Nein	*Fundstelle*
Werden die erfassten Daten von einer zweiten Person, die weder an der Datenermittlung noch an der Datenerfassung beteiligt gewesen ist, geprüft (Vier-Augen-Prinzip)?	Ja/Nein	*Fundstelle*
Hinweis: *Die nachfolgenden Fragen sind nur zu beantworten, wenn die vorherige Frage mit „Ja“ beantwortet wird.*		
Ist technisch gewährleistet, dass die prüfende Person die erfassten Daten nicht verändern kann?	Ja/Nein	*Fundstelle*
Wird die Prüfung der Datenerfassung unter Beachtung der Vorgaben nach Nr. 5.4 VerfRi-IT-HKR bescheinigt?	Ja/Nein	*Fundstelle*
Werden die Daten, wenn bei der Prüfung Fehler festgestellt werden, von einer zur Datenerfassung befugten Person berichtigt und von einer zweiten, dafür berechtigten Person erneut geprüft?	Ja/Nein	*Fundstelle*

b) Datenerfassung durch Übernahme elektronischer Daten

Erfolgt eine Datenerfassung durch Übernahme elektronischer Daten?	Ja/Nein	*Fundstelle*
Hinweis: *Die nachfolgenden Fragen sind nur zu beantworten, wenn die vorherige Frage mit „Ja“ beantwortet wird.*		
Wird die vollständige und richtige Datenübernahme manuell oder maschinell kontrolliert?	Ja/Nein	*Fundstelle*

Werden die Kontrollen dokumentiert?	Ja/Nein	*Fundstelle*
Ist die sachliche und rechnerische Richtigkeit der übernommenen Daten durch die Behörde, die die Daten übergibt, bescheinigt?	Ja/Nein	*Fundstelle*
Hinweis: *Die nachfolgenden Fragen sind nur zu beantworten, wenn die vorherige Frage mit „Nein“ beantwortet wird.*		
Wird die sachliche und rechnerische Richtigkeit der übernommenen Daten durch einen Sachbearbeiter bescheinigt?	Ja/Nein	*Fundstelle*
Erfolgt die Bescheinigung nach den Vorgaben der Nr. 5.3 VerfRi-IT-HKR?	Ja/Nein	*Fundstelle*
Werden die erfassten Daten von einer zweiten Person, die weder an der Datenermittlung noch an der Datenerfassung beteiligt gewesen ist, geprüft (Vier-Augen-Prinzip)?	Ja/Nein	*Fundstelle*
Hinweis: *Die nachfolgenden Fragen sind nur zu beantworten, wenn die vorherige Frage mit „Ja“ beantwortet wird.*		
Ist technisch gewährleistet, dass die prüfende Person die erfassten Daten nicht verändern kann?	Ja/Nein	*Fundstelle*
Wird die Prüfung der Datenerfassung unter Beachtung der Vorgaben nach Nr. 5.4 VerfRi-IT-HKR bescheinigt?	Ja/Nein	*Fundstelle*
Werden die Daten, wenn bei der Prüfung Fehler festgestellt werden, von einer zur Datenerfassung befugten Person berichtigt und von einer zweiten, dafür berechtigten Person erneut geprüft?	Ja/Nein	*Fundstelle*

c) Datenübertragung an IT-Verfahren nach VV Nr. 6.1.1 zu §§ 70-80 LHO M-V

Findet eine Übertragung von Daten aus dem IT-Verfahren an das HKR-Verfahren statt?	Ja/Nein	*Fundstelle*
Hinweis: *Die nachfolgende Frage ist nur zu beantworten, wenn die vorherige Frage mit „Ja“ beantwortet wird.*		
Enthalten die übertragenen Daten Informationen, mit denen der Sachbearbeiter identifiziert werden kann, der die Daten freigegeben oder angeordnet hat?	Ja/Nein	*Fundstelle*
Wird die richtige und vollständige Datenübertragung durch systemtechnische Kontrollen (z.B. Saldenabgleich) überprüft?	Ja/Nein	*Fundstelle*

Findet eine Übertragung von Daten aus dem IT-Verfahren an das Zahlungsverkehrsverfahren statt?	Ja/Nein	*Fundstelle*
Hinweis: *Die nachfolgende Frage ist nur zu beantworten, wenn die vorherige Frage mit „Ja“ beantwortet wird.*		
Enthalten die übertragenen Daten Informationen, mit denen der Sachbearbeiter identifiziert werden kann, der die Daten freigegeben oder angeordnet hat?	Ja/Nein	*Fundstelle*

Wird die richtige und vollständige Datenübertragung durch systemtechnische Kontrollen (z.B. Saldenabgleich) überprüft?	Ja/Nein	*Fundstelle*

5. Protokollierung und Revisionsfähigkeit (Nr. 5.8 VerfRi-IT-HKR)

Erfolgt ein sachlicher und zeitlicher Nachweis über alle buchführungspflichtigen Geschäftsvorfälle?	Ja/Nein	*Fundstelle*
Ist der Nachweis dahingehend prüfbar, ob die materiellen Anforderungen an eine Ein- oder Auszahlung erfüllt bzw. die Buchungen inhaltlich richtig sind?	Ja/Nein	*Fundstelle*
Kann die Prüfung von einem Sachverständigen in angemessener Zeit vorgenommen werden?	Ja/Nein	*Fundstelle*
Werden Zugriffe auf das IT-Verfahren dokumentiert?	Ja/Nein	*Fundstelle*
Kann nachgewiesen werden, welche Person (insbesondere Anwender und Administratoren) zu welcher Zeit welche Aktionen angestoßen und ausgeführt hat?	Ja/Nein	*Fundstelle*
Enthält der Nachweis die geänderten Daten mit altem und neuem Stand?	Ja/Nein	*Fundstelle*
Werden die vorgenommenen Buchungen und ihre Reihenfolge durch einen Beleg dokumentiert?	Ja/Nein	*Fundstelle*
Enthält der Beleg (Nachweis über Buchung) zum Buchungsvorgang • eine hinreichende Erläuterung des Vorgangs, • den zu buchenden Betrag, • den Zeitpunkt des Vorgangs und • die Bescheinigungen über die Datenerfassung und Datenfreigabe?	Ja/Nein	*Fundstelle*
Ist – auch im Falle eines Medienbruchs – gewährleistet, dass die zahlungsbegründenden Unterlagen dem Beleg und umgekehrt die Belege den Unterlagen zugeordnet werden können?	Ja/Nein	*Fundstelle*
Sind die Nachweise und Belege nach ihrer Erstellung unveränderbar?	Ja/Nein	*Fundstelle*
Können die Geschäftsvorfälle vollständig oder auszugsweise sowie geordnet nach Zeitpunkt, Sach- und Personenkonten dargestellt werden?	Ja/Nein	*Fundstelle*
Ist eine Prüferrolle eingerichtet, die einen lesenden Zugriff auf alle Daten und Systemeinstellungen des IT-Verfahrens ermöglicht?	Ja/Nein	*Fundstelle*

6. IT-Sicherheit (Nr. 5.9 VerfRi-IT-HKR)

Sind Vorkehrungen gegen den Verlust, die mehrfache Verarbeitung und die Manipulation gespeicherter Daten sowie gegen Systemfehler getroffen worden?	Ja/Nein	*Fundstelle*

Liegt für das IT-Verfahren ein Sicherheitskonzept gemäß IT-Grundschutz des Bundesamtes für Sicherheit und Informationstechnik (BSI) vor?	Ja/Nein	*Datum und Version*
Ist das IT-Verfahren durch die verantwortliche Stelle freigegeben?	Ja/Nein	*Datum und Aktenzeichen der Erteilung*
Ist durch Wartungsverträge oder auf andere Weise sichergestellt, dass Programmfehler oder Sicherheitslücken des IT-Verfahrens in angemessener Zeit beseitigt werden können?	Ja/Nein	*Fundstelle*

7. Regelungen für Anwender

Enthält die Verfahrensdokumentation/Dienstanweisung für das IT-Verfahren Vorgaben		
• für den Zugriff auf das Verfahren?	Ja/Nein	*Fundstelle*
• für die Datenerfassung und -freigabe?	Ja/Nein	*Fundstelle*
• zur IT-Sicherheit?	Ja/Nein	*Fundstelle*
• zur Einhaltung des Berechtigungskonzepts?	Ja/Nein	*Fundstelle*
• zur Archivierung von Rechnungsbelegen?	Ja/Nein	*Fundstelle*

8. Interne Prüfungen (Nr. 5 Anlage 6 zu §§ 70-80 LHO M-V)

Ist ein Verfahren festgelegt, wie die Einhaltung der kassenrechtlichen Vorschriften geprüft wird?	Ja/Nein	*Fundstelle*
Ist eine verantwortliche Person für die Prüfungen festgelegt?	Ja/Nein	*Fundstelle*
Sind verbindliche Zeiträume für die einzelnen Prüfungen festgelegt?	Ja/Nein	*Fundstelle*
Ist eine Prüfung vorgeschrieben, ob das eingesetzte IT-Verfahren dem dokumentierten und genehmigten Verfahren entspricht?	Ja/Nein	*Fundstelle*
Ist die Dokumentation der Prüfungen vorgeschrieben?	Ja/Nein	*Fundstelle*

9. Manuelle Verfahrensschritte außerhalb des IT-Verfahrens

Erfolgen die Feststellung der sachlichen und rechnerischen Richtigkeit oder die Anordnung schriftlich?	Ja/Nein	*Fundstelle*
Hinweis: *Die nachfolgenden Fragen sind nur zu beantworten, wenn die vorherige Frage mit „Ja“ beantwortet wird.*		
Bescheinigt ein Sachbearbeiter die sachliche und rechnerische Richtigkeit durch Unterschrift?	Ja/Nein	*Fundstelle*
Erfolgt die Anordnung durch einen Sachbearbeiter/Vorgesetzten, der entsprechend befugt ist und nicht zugleich die rechnerische und/oder sachliche Richtigkeit bescheinigt hat (Vier-Augen-Prinzip)?	Ja/Nein	*Fundstelle*

Bescheinigt ein Sachbearbeiter/Vorgesetzter die Anordnung durch Unterschrift?	Ja/Nein	*Fundstelle*
Erfolgen sonstige Verfahrensschritte manuell?	Ja/Nein	*Fundstelle*
Hinweis: *Die nachfolgende Frage ist nur zu beantworten, wenn die vorherige Frage mit „Ja“ beantwortet wird.*		
Werden bei den manuellen Verfahrensschritten die kassenrechtlichen Vorschriften, insbesondere die Anlage 2 zu §§ 70-80 LHO M-V eingehalten?	Ja/Nein	*Fundstelle*

10. Archivierung von Unterlagen

a) Papiergestützte Archivierung

Erfolgt eine papiergestützte Archivierung von Belegen und zahlungsbegründenden Unterlagen oder Nachweisen (nachfolgend: Belege)?	Ja/Nein	*Fundstelle*
Hinweis: *Die nachfolgenden Fragen sind nur zu beantworten, wenn die vorherige Frage mit „Ja“ beantwortet wird.*		
Werden die Belege bei der nach VV Nr. 4.7 zu §§ 70-80 LHO M-V zuständigen Stelle aufbewahrt?	Ja/Nein	*Fundstelle*
Sind die Belege gegen Verlust, Beschädigung und den Zugriff Unbefugter gesichert?	Ja/Nein	*Fundstelle*
Werden die Belege getrennt nach Haushaltsjahren aufbewahrt?	Ja/Nein	*Fundstelle*
Wird die Haltbarkeit und Lesbarkeit der Belege jährlich geprüft?	Ja/Nein	*Fundstelle*
Ist ein sachverständiger Dritter in angemessener Zeit in der Lage, gezielt auf einzelne sowie zusammenhängende Belege zuzugreifen?	Ja/Nein	*Fundstelle*
Ist die Archivierung der Belege für die Dauer der kassenrechtlichen Aufbewahrungsfristen nach VV Nr. 4.7 zu §§ 70-80 LHO M-V gewährleistet?	Ja/Nein	*Fundstelle*

b) Elektronische Archivierung (Nr. 6 der Anlage 6 zu §§ 70-80 LHO M-V)

Erfolgt eine ausschließlich elektronische Archivierung von Belegen und zahlungsbegründenden Unterlagen oder Nachweisen (nachfolgend: Belege)?	Ja/Nein	*Fundstelle*
Hinweis: *Die nachfolgende Frage ist nur zu beantworten, wenn die vorherige Frage mit „Ja“ beantwortet wird.*		
Wird für die Archivierung der Belege ein sicheres Verfahrens genutzt?	Ja/Nein	*Fundstelle*
Hinweis: *Die nachfolgenden Fragen sind nur zu beantworten, wenn die vorherige Frage mit „Nein“ beantwortet wird.*		
Werden die Belege unveränderbar auf einem Datenträger gespeichert?	Ja/Nein	*Fundstelle*

Werden die Belege in einer vorgegebenen Struktur archiviert?	Ja/Nein	*Fundstelle*
Ist die Archivierung der Belege für die Dauer der kassenrechtlichen Aufbewahrungsfristen gemäß VV Nr. 4.7 zu §§ 70-80 LHO M-V gewährleistet?	Ja/Nein	*Fundstelle*
Sind die Verfahrensabläufe für die Archivierung der Belege in der Verfahrensdokumentation bzw. in einer Dienstanweisung geregelt?	Ja/Nein	*Fundstelle*
Können die Belege lesbar gemacht und ausgedruckt werden?	Ja/Nein	*Fundstelle*
Ist ein gezielter Zugriff auf einzelne Belege möglich?	Ja/Nein	*Fundstelle*
Können zusammenhängende Belege zusammengeführt werden?	Ja/Nein	*Fundstelle*
Ist ein sachverständiger Dritter in angemessener Zeit in der Lage, gezielt auf einzelne sowie zusammenhängende Belege zuzugreifen?	Ja/Nein	*Fundstelle*
Wird die Lesbarkeit der Belege in regelmäßigen Abständen kontrolliert?	Ja/Nein	*Fundstelle*

c) Übertragung von schriftlichen Unterlagen in elektronische Form (Nr. 6.4 der Anlage 6 zu §§ 70-80 LHO M-V)

Erfolgt eine Übertragung von Rechnungsbelegen in eine elektronische Form?	Ja/Nein	*Fundstelle*
Hinweis: *Die nachfolgenden Fragen sind nur zu beantworten, wenn die vorherige Frage mit „Ja“ beantwortet wird.*		
Wird die Vollständigkeit und Richtigkeit der Übertragung der Belege in die elektronische Form durch entsprechende Kontrollen gewährleistet?	Ja/Nein	*Fundstelle*
Werden diese Kontrollen protokolliert?	Ja/Nein	*Fundstelle*
Ist gewährleistet, dass im Falle einer Übertragung die schriftlichen Rechnungsbelege eines Haushaltsjahres frühestens nach Ablauf des Jahres vernichtet werden, in dem die Entlastung für dieses Haushaltsjahr erteilt worden ist?	Ja/Nein	*Fundstelle*
Sind die Verfahrensabläufe für die Übertragung der Belege in der Verfahrensdokumentation/einer Dienstanweisung geregelt?	Ja/Nein	*Fundstelle*

11. Gefährdungsanalyse

Werden die aus den Abweichungen von den kassenrechtlichen Vorschriften resultierenden Risiken in der Gefährdungsanalyse dargestellt und bewertet?	Ja/Nein	*Fundstelle*
Sind sämtliche aufgeführten Risiken für die Kassensicherheit beherrschbar?	Ja/Nein	*Fundstelle*

Wird regelmäßig geprüft, ob die Angaben in der Gefährdungsanalyse zutreffend sind (Risikokontrolle)?	Ja/Nein	*Fundstelle*
Ist in der Gefährdungsanalyse eine verantwortliche Person für die Risikokontrolle benannt?	Ja/Nein	*Fundstelle*

12. Stichprobenkontrollverfahren

Hinweis: *Die nachfolgende Frage ist nur zu beantworten, wenn die Richtigkeit und Vollständigkeit der Datenerfassung nicht im Vier-Augen-Prinzip geprüft.*		
Wird die Richtigkeit und Vollständigkeit der Datenerfassung in einem Stichprobenkontrollverfahren überprüft?	Ja/Nein	*Fundstelle*
Hinweis: *Die nachfolgenden Fragen sind nur zu beantworten, wenn die vorherige Frage mit „Ja“ beantwortet wird.*		
Handelt es sich um ein Stichprobenkontrollverfahren nach den Vorgaben der Nr. 5.4.6 VerfRi-IT-HKR?	Ja/Nein	*Fundstelle*
Werden die im Rahmen der Stichprobenprüfung zu kontrollierenden Fälle vor der Freigabe der Daten geprüft?	Ja/Nein	*Fundstelle*
Ist gewährleistet, dass die weitere Bearbeitung der Daten der Stichprobe bis zum Abschluss der Prüfung ausgeschlossen ist?	Ja/Nein	*Fundstelle*
Ermöglicht das IT-Verfahren die freie Einstellung der Parameter, die Auswirkungen auf die quantitative und qualitative Zusammensetzung der Stichprobe haben?	Ja/Nein	*Fundstelle*
Gibt es ein Verfahren, in dem die für die Kassensicherheit besten Parameterwerte bestimmt werden?	Ja/Nein	*Fundstelle*
Können Änderungen der Parameter nur mit Zustimmung des Beauftragten für den Haushalt oder seiner bevollmächtigten Person erfolgen?	Ja/Nein	*Fundstelle*
Werden Änderungen der Parameter dokumentiert?	Ja/Nein	*Fundstelle*
Wird regelmäßig untersucht, ob die Zusammensetzung der Stichprobe zur Gewährleistung der Kassensicherheit geändert werden muss?	Ja/Nein	*Fundstelle*
Werden die bei der Stichprobenprüfung festgestellten Fehler dokumentiert?	Ja/Nein	*Fundstelle*
Gibt es für das Stichprobenkontrollverfahren ein Fehlermanagement und ein Berichtswesen?	Ja/Nein	*Fundstelle*
Wird regelmäßig auf Grundlage der in den Stichproben aufgetretenen Fehlerkonstellationen geprüft, ob eine Änderung der Parameterwerte erforderlich ist?	Ja/Nein	*Fundstelle*
Ist das Stichprobenkontrollverfahren in einer Dienst- oder Fachanweisung geregelt?	Ja/Nein	*Fundstelle*

13. Sonstige Abweichungen von kassenrechtlichen Vorschriften

Sind aus der förmlichen Anordnung und ihren Anlagen Zweck und Anlass der Ein- oder Auszahlung deutlich erkennbar (Begründung: Grund, Rechtsgrund, Berechnung etc.)?	Ja/Nein	*Fundstelle*
Werden die übrigen kassenrechtlichen Anforderungen der VV zu §§ 70-80 LHO M-V und Anlagen (insbesondere Anlage 6) erfüllt?	Ja/Nein	*Fundstelle*