



Gemeindeprüfungsanstalt
Baden-Württemberg

GPA-Mitteilung 1/2012

Az. 049.00

15.03.2012

Einsatz von autonomen ADV-Verfahren im Finanzwesen

1 Ausgangslage

An ADV-Verfahren (Programmen) zur Abwicklung von Finanzvorgängen und deren Einsatz in den Verwaltungen stellt das Haushalts- und Kassenrecht hohe Anforderungen. Für automatisierte Verfahren sind „besondere“ Regelungen¹ getroffen worden, denn mit den Programmen werden öffentliche Gelder zu treuen Händen verwaltet. Die finanzwirksamen Programme müssen deshalb die Kommune nicht nur bei der Aufgabenerledigung unterstützen, sondern die ordnungsmäßige Abwicklung „sicherstellen“.² Dieses Sicherstellen bezieht sich nicht nur auf das Programm i. S. einer richtigen Programmierung, sondern auch auf seine Ausgestaltung (Customizing) und den technischen Programmeinsatz (sicherer Rechnerbetrieb usw.).

Die besonderen Anforderungen spiegeln sich auch im Prüfungsrecht wider. Zum einen in den Regelungen zur Programmprüfung (Pflichtprüfung nach § 114a Abs. 1 GemO) und zum anderen in den Vorgaben zur sogen. Anwendungsprüfung im Rahmen der örtlichen bzw. überörtlichen Finanzprüfung (§ 6 Abs. 2 Nr. 11 GemPrO).

Die Anforderungen, die an die Programme und den Programmeinsatz gestellt werden, bestehen unabhängig davon, ob die Kommune sich eines Regionalen Rechenzentrums bedient oder autonome Verfahren einsetzt. Wendet eine Kommune die vom DV-Verbund (Datenzentrale, Regionalen Rechenzentren) angebotenen Verfahren an, so übernimmt der DV-Verbund für die Kommune die Verantwortung für die übertragenen Leistungen. Zudem wird die Kommune kraft Gesetzes von einzelnen Aufgaben entbunden. Betreibt die Kommune hingegen eine autonome Lösung, so ist sie insgesamt **eigenverantwortlich** tätig.

¹ Insbesondere § 6 GemKVO und § 35 Abs. 5 und 6 GemHVO.

² Z. B. notwendiger hoher Grad an automatisierten Kontrollen (z. B. Plausibilitätsprüfungen, Abstimmprogramme).

Nachfolgend wird dargelegt, welche Folgen der Einsatz autonomer Verfahren (hier insbesondere zentraler Finanzsoftware mit Buchführung, Veranlagung und ggf. Personalabrechnung) im Vergleich zur Anwendung der Programme des DV-Verbands hat. Dabei werden die Anforderungsbereiche „Ordnungsmäßigkeit des Programms“ (ordnungsmäßige Programmierung und Ausgestaltung des Programms i. S. vom Customizing) und „Ordnungsmäßiger Programmeinsatz“ (Rechnerbetrieb usw.) unterschieden.

2 Anforderungsbereich „Ordnungsmäßigkeit des Programms“

2.1 Kassenrechtliche Programmfreigabe

2.1.1 Grundsatz

Verantwortlich für das eingesetzte ADV-Verfahren ist aus kassen- bzw. haushaltsrechtlicher Sicht nicht der „Programmierer“ (Programmersteller), sondern die das Programm einsetzende Kommune.¹ Die Kommune muss sich Fehler des Programms zurechnen lassen. Fehlerhafte Programmresultate können durch eine fehlerhafte Programmiervorgabe oder eine nicht sachgerechte Umsetzung dieser Vorgabe im Rahmen der Programmierung (Codierung) bzw. Ausgestaltung des Programms (Customizing) entstehen.

Vor diesem Hintergrund ist die **kassenrechtlich Programmfreigabe**² (§ 6 GemKVO, § 35 Abs. 5 Nr. 1 GemHVO) **grundlegende Voraussetzung für den Programmeinsatz**. Diese besteht aus

- a) den konkreten Freigabehandlungen (z. B. Austesten von Programmfunktionen), um die Ordnungsmäßigkeit des Programms festzustellen und
- b) der darauf aufbauenden formalen Freigabeerklärung.

Erst auf dieser Grundlage darf das Programm eingesetzt werden. Im Sonderheft 1/2010 der GPA-Mitteilungen ist ausführlich auf die kassenrechtliche Programmfreigabe hingewiesen worden.

¹ Vgl. hierzu auch die Tz. 9 der Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) BMF IV A 8 – S 0316 - 43/95 -; BStBl. I 1995, 738 ff.

² Zuständig für die Programmfreigabe ist gemäß § 35 Abs. 5 Nr. 1 GemHVO der Bürgermeister bzw. die von ihm bestimmte Stelle.

2.1.2 Verfahren des DV-Verbunds

Nutzt eine Kommune die Verfahren des DV-Verbunds, so wird die Datenzentrale bzw. das Regionale Rechenzentrum als sogen. andere amtliche Stelle tätig (zur Sonderstellung des DV-Verbunds siehe auch Ziffer 2.2.2). Der DV-Verbund übernimmt die konkrete **Handlungsverantwortung für das Programm und den Programmeinsatz**. Sie wird zwischen Rechenzentrum und Kommune formal durch das einmalige Erteilen der Einsatzbescheinigung und das jährliche Erteilen der (Teil-)Feststellungsbescheinigungen¹ wahrgenommen. Bei der Kommune verbleiben lediglich die Verantwortungen für die **Programmanwendung** und (soweit relevant) für die **individuellen Verfahrensausprägungen** (z. B. falls der Anwender selbst Customizingeinstellungen durchführt).

Die Grundlage der Einsatzbescheinigung basiert auf einem definierten Projektfreigabeprozess² des DV-Verbunds, der konkret vorgegebene Handlungsanweisungen (z. B. notwendige Tests bei Releasewechsel mit Testplänen usw.) enthält. Hinzu kommt, dass im Rahmen dieser Projektfreigabe einzelne Anwender stellvertretend für die übrigen Kommunen mit eingebunden sind (fachlicher Input als Bestandteil der Programmiervorgabe). Die GPA ist im Rahmen der **begleitenden Programmprüfung** bereits bei der Erarbeitung der Programmiervorgaben (Lastenhefte der Rechenzentren bzw. Pflichtenhefte der Datenzentrale) und damit bei dem Projektfreigabeprozess frühzeitig und unmittelbar beteiligt. Der DV-Verbund gibt insoweit der GPA „Gelegenheit, Prüfungshandlungen bereits bei der Vorbereitung des Programmeinsatzes vorzunehmen“ (§ 114a Abs. 1 Satz 4 GemO).

Daneben ist der DV-Verbund nicht nur Hersteller bzw. Anbieter von (Standard-)Software, sondern bietet auch Verfahrensausprägungen an (z. B. Kommunalmasterkonzept bei SAP, Modellkommune bei KIRP). Insoweit nutzt der Anwender nicht nur (Standard-)Software, sondern eine bestimmte Verfahrensausprägung, die diesen Projektfreigabeprozess durchlaufen hat.

Die einzelne Kommune partizipiert somit unmittelbar an dem Projektfreigabeprozess der **Solidargemeinschaft DV-Verbund** und kann sich bei ihrer kassenrechtlichen Programmfreigabe auf die erteilte Einsatzbescheinigung berufen. Die Kommune kann auf eigene Freigabehandlungen weitestgehend verzichten, wenn sie sich an die festgelegten „Standards“ (wie Kommunalmasterkonzept, Modellkommune) des DV-Verbunds hält.

2.1.3 Autonome Verfahren

Bei autonomen Verfahren werden i. d. R. keine Anwendergemeinschaften (i. S. einer Solidargemeinschaft) gebildet. Wenn überhaupt, sind nur lose Anwendergruppen vorhanden. Zwar durchlaufen bei jedem Programmhersteller die Softwareprojekte einen in sich definierten dv-technischen Freigabeprozess (teilweise sogar von Dritten zertifiziert). Allerdings fehlt i. d. R. ein

¹ Siehe hierzu GPA-Mitt. 5/2010 Az. 910.00, Einsatz- und (Teil-)Feststellungsbescheinigung bei der Anwendung von ADV-Verfahren zur Abwicklung von Finanzvorgängen.

² Hier ist das Projekt „Softwareentwicklung“ gemeint (gesamtes Programm, neues Release, einzelne Funktionalität). Die Abläufe sind im DV-Verbund u. a. über das sogen. Anforderungsmanagement geregelt.

autorisiertes „Anwendergremium“, das in Vertretung der übrigen (baden-württembergischen) Anwender die fachlichen Programmervorgaben mitgestaltet, die GPA-Programmprüfung einbindet und den Programmentwicklungsprozess fachlich überwacht.

Beim Einsatz autonomer Finanzsoftware ist die **Kommune selbst verantwortlich**. Dies führt bei jeder einzelnen Kommune zu einem Freigabeaufwand (eigene Tests vor Programmeinsatz bzw. vor Einsatz neuer Releases, Vorhalten entsprechender Testsysteme mit Schnittstellenanbindungen usw.).¹

Eine Sonderform stellt das **Hosting** dar. In diesem Fall nutzt die Kommune als autonome Anwenderin die technische Infrastruktur eines Rechenzentrums und lagert quasi ihren Rechner in das Rechenzentrum aus bzw. nutzt die dortige Rechnerleistung. Da das Rechenzentrum beim reinen Hosting keine Programmverantwortung übernimmt, bezieht sich die Einsatzbescheinigung des Rechenzentrums lediglich auf den tatsächlichen Rechnerbetrieb und nicht auf das eigentliche Programm. Die kassenrechtliche Programmfreigabe kann sich insoweit in Bezug auf die Ordnungsmäßigkeit des Programms nicht auf eine erteilte Einsatzbescheinigung stützen.

Die im Zusammenhang mit der Freigabe notwendigen Handlungen verursachen bei jeder Kommune zwangsläufig zusätzlichen Aufwand.

2.2 Programmprüfung

2.2.1 Grundsatz

Die Programmprüfung nach § 114a GemO unterscheidet beim Prüfungsverfahren zwischen Programmen des DV-Verbunds und sogen. autonomen Programmen. Die Datenzentrale bzw. die Regionalen Rechenzentren übernehmen als Programmanbieter konkrete Aufgaben im Programmprüfungsverfahren für die von ihnen betreuten Kommunen. Hinsichtlich der Frage einer eventuellen Prüfungspflicht (Pflichtprüfung nach § 114a Abs. 1 Satz 1 GemO²) und der „Art und Weise“ der Prüfung (Prüfungsanforderungen, Prüfungstiefe) werden die Verfahren des DV-Verbunds und autonome Verfahren gleich behandelt. Auch ist es unerheblich, ob ein Programm nur bei wenigen Anwendern oder (nahezu) flächendeckend im Einsatz ist.

2.2.2 Verfahren des DV-Verbunds

Beim Einsatz von Programmen des DV-Verbunds hat die Kommune, in Bezug auf die Programmprüfung, keine Verpflichtungen. Diese obliegen dem DV-Verbund als Programmanbieter i. S. des § 114a Abs. 1 Satz 2 GemO. Gebührenschuldner der Prüfungskosten ist der DV-Verbund, der diese über Umlagen bzw. Fallpreise auf die einzelnen Anwender solidarisch verteilt. Die Kommune partizipiert insoweit an der Solidargemeinschaft DV-Verbund.

¹ Im Sonderheft 1/2010 der GPA-Mittelungen, Freigabe von ADV-Verfahren wird detailliert beschrieben, wie sich der autonome Programmeinsatz auf die Freigabehandlungen auswirkt.

² Zur Abgrenzung der prüfungspflichtigen Programme siehe GPA-Mitt. 3/2006 Az. 095.90.

2.2.3 Autonome Verfahren

Die Kommune ist bei autonomen Verfahren selbst **Adressat der Programmprüfung**. Ihr obliegt die sogen. Veranlassungspflicht, welche die Meldepflicht der prüfungspflichtigen autonomen Programme an die GPA, sowie eine Mitwirkungspflicht bei der Programmprüfung beinhaltet (§ 114a Abs. 1 Satz 2 GemO). So muss die Kommune die technischen Voraussetzungen schaffen, damit die Prüfung erfolgen kann (Einrichten eines Testmandanten, Vorbereiten eines Testdatenbestands, Bereitstellen der Programmdokumentation usw.).

Die **Kosten der Programmprüfung** sind unmittelbar von der Kommune zu tragen, die das Programm einsetzt. Die Kommune trägt damit ein Kostenrisiko, weil die Prüfungsdauer und die Prüfungskosten auch von der „Art“ der Software (z. B. hohe Komplexität durch eine Vielzahl von Verfahrensausprägungen) und deren Güte (z. B. Aussagefähigkeit, Vollständigkeit der Programmdokumentation) abhängen. Eine Kostenübernahme durch den Programmhersteller muss die Kommune vertraglich vereinbaren. Daneben ist sie der Adressat des Prüfungsberichts der Programmprüfung; die Kommune hat dafür Sorge zu tragen, dass festgestellte Fehler vom Programmhersteller ausgeräumt werden.

3 Anforderungsbereich „Ordnungsmäßiger Programmeinsatz“

3.1 Sicherstellung Daten- und Programmsicherheit

3.1.1 Grundsatz

Nach § 6 GemKVO, § 35 Abs. 5 und 6 GemHVO i. V. m. den Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) werden an finanzwirksame ADV-Verfahren **hohe Anforderungen in Bezug auf die Daten- und Programmsicherheit** gestellt. Es obliegt hierbei dem Bürgermeister, die notwendigen Sicherheitsvorkehrungen zu treffen (§ 35 Abs. 6 Satz 1 GemHVO).

3.1.2 Verfahren des DV-Verbunds

Das Rechenzentrum führt die erforderlichen Maßnahmen durch (bis hin zu Notfallplänen mit Einrichten eines Ausweichrechenzentrums usw.). Die Kommune stützt sich auf die erteilte Einsatzbescheinigung (siehe oben Ziffer 2.1.2).

3.1.3 Autonome Verfahren

Die Kommune betreibt im Rahmen der Inhouse-Verarbeitung ihr eigenes Rechenzentrum. Sie ist dafür verantwortlich, die Risiken (z. B. durch höhere Gewalt, organisatorische Mängel,

menschliche Fehlhandlungen, technisches Versagen, Risiken von außen über Internet usw.) richtig zu bewerten und die notwendigen Maßnahmen zu treffen.

Grundlage der Risikobewertung ist eine **Schwachstellenanalyse**.¹ Diese sollte nach den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) vorgenommen werden. Die aufgezeigten Schwachstellen sind anschließend zu bewerten und darauf aufbauend, sind die notwendigen Maßnahmen einzuleiten. Dabei sind grundsätzlich vier Handlungsalternativen denkbar:

- a) Das Risiko wird durch weitere Sicherheitsmaßnahmen reduziert (z. B. Sicherheitstür, Sicherheitsverglasungen, Rauch- und Wassermelder im Rechnerraum, Auslagerung von Datensicherungsbeständen).
- b) Das Risiko wird vermieden (z. B. Verlagerung des Rechnerraums vom UG zum OG und damit Vermeidung einer Gefährdung durch Hochwasser).
- c) Das Risiko wird verlagert (z. B. durch den Abschluss von Versicherungen). Hierbei ist grundsätzlich zu hinterfragen, ob eine monetäre Absicherung ausreichend ist (Datenverlust kann u. U. nicht „ersetzt“ werden). Eine gezielte Verlagerung des Risikos erfolgt beispielsweise durch das Hosting (siehe auch oben Ziffer 2.1.3).²
- d) Das Risiko wird übernommen, die Kommune (der Bürgermeister) akzeptiert das Risiko. Der Bürgermeister übernimmt dafür die Verantwortung.

Nicht thematisiert wird hier bewusst die Frage, inwieweit die jeweilige Kommune in der Lage ist, bei Inhouse-Verarbeitung ein vergleichbares Sicherheitsniveau wie bei einem (zentralen) Rechenzentrumsbetrieb zu erreichen (z. B. sicherer Closed-Shop-Betrieb). Bei der Risikoabschätzung und den damit verbundenen erforderlichen Maßnahmen wird selbstverständlich zu unterscheiden sein, ob die Kommune lediglich einen „kleinen“ Finanzbereich eigenständig abdeckt (z. B. Friedhofwesen) oder ihre komplette Buchführung (einschließlich der zentralen Veranlagungsverfahren und ggf. auch der Personalabrechnung) selbständig abwickelt.

Es ist zu beachten, dass eine Inhouse-Verarbeitung speziell **ausgebildete DV-Spezialisten** erfordert. Vertretungen müssen bestellt und diese müssen entsprechend geschult sein. Da die Datenverarbeitung einem stetigen Wandel unterliegt, sind laufende Fortbildungsmaßnahmen sowohl in der allgemeinen DV-Technik (Betriebssystem, Datenbank usw.), als auch in Bezug auf die eingesetzten Anwendungsprogramme unerlässlich. Da die Mitarbeiter der DV-Abteilung i. d. R. nicht über das erforderliche fachliche Spezialwissen verfügen (können), kann die DV-Abteilung auch nur die ordnungsgemäße dv-technische Verarbeitung der Daten sicherstellen. Beim Programmeinsatz in Eigenregie muss die fachliche Seite deshalb vom Fachamt, von der Kämmerei bzw. der Kasse abgedeckt werden (z. B. Beurteilung der Notwendigkeit von Pro-

¹ Siehe hierzu auch GPA-Mitt. 1/2010 Az. 049.00, Einsatz von ADV-Verfahren in Eigenregie.

² Die Kommune kann sich beim Hosting in Bezug auf die Daten- und Programmsicherheit dann auf die vom Rechenzentrum erteilte Einsatzbescheinigung stützen.

grammupdates, Erarbeiten von Testfällen und Austesten der Funktionen vor dem Einsatz einer neuen Programmversion).

Die erforderlichen Maßnahmen zu treffen bedeutet auch, dass die dafür notwendigen monetären Aufwendungen zu tragen sind. Der wirtschaftliche Einsatz einer Finanzsoftware darf nicht auf Kosten der Sicherheit und damit der Ordnungsmäßigkeit erfolgen.

Exkurs Datenschutzrecht

Die Einhaltung der datenschutzrechtlichen Bestimmungen ist nicht Gegenstand der GPA-Prüfung. Allerdings darf die Problematik des Datenschutzes nicht unerwähnt bleiben. Zwar sind bzgl. der Daten- und Programmsicherheit die Anforderungen aus datenschutzrechtlicher Sicht in weiten Teilen mit den haushalts- und kassenrechtlichen Vorgaben deckungsgleich. Allerdings kommen spezielle Anforderungen, wie z. B. Löschpflichten bei personenbezogenen Daten hinzu. Während im Haushalts- und Kassenrecht der Fokus auf die Änderung (auch i. S. von Manipulation) von finanzwirksamen Daten gerichtet ist, ist im Bereich des Datenschutzes bereits der unberechtigte lesende Zugriff auf (personenbezogene) Daten sicherheitsrelevant. Hinzu kommen sonstige Pflichten aus dem Landesdatenschutzgesetz bzw. aus weiteren Spezialgesetzen. Um diesen Anforderungen gerecht zu werden, dürfte es generell angebracht sein, einen örtlichen Datenschutzbeauftragten (§ 10 LDSG) zu bestellen.

3.2 Prüfung der Daten- und Programmsicherheit

3.2.1 Grundsatz

Die Sicherstellung einer ausreichenden Daten- und Programmsicherheit beim Einsatz von Finanzsoftware ist grundsätzlich Bestandteil der örtlichen und überörtlichen Finanzprüfung (§ 6 Abs. 2 Nr. 11 GemPrO).

3.2.2 Verfahren des DV-Verbunds

Erfolgt die Datenverarbeitung beim Regionalen Rechenzentrum, so deckt bereits die Programmprüfung durch die GPA den Bereich der Daten- und Programmsicherheit mit ab (Prüfung der Ordnungsmäßigkeit der Anwendung an Ort und Stelle gemäß § 114a Abs. 1 Satz 4 GemO).

Die örtliche bzw. überörtliche (Finanz-) Prüfung nimmt keine eigenen Prüfungshandlungen beim Rechenzentrum vor.

3.2.3 Autonome Verfahren

Bei Inhouse-Verarbeitung autonomer Verfahren ist eine zentrale (Vor-) Prüfung nicht möglich. Insoweit muss die Anwendungs- und Programmsicherheitsprüfung bei jeder einzelnen Kommune dezentral durchgeführt werden. Für die mit der Aufgabe betrauten Prüfer/Prüferinnen bedeu-

tet dies, dass sie sich dv-technisch in verschiedenen Programmen vertieft aus- bzw. fortbilden müssen.

Erfahrungen aus der überörtlichen Prüfung zeigen, dass der Sicherheitsproblematik einer In-house-Verarbeitung oft nicht die erforderliche Bedeutung beigemessen wird (z. B. fehlende Schwachstellen- bzw. Risikoanalyse). Die GPA ist deshalb beim Einsatz autonomer zentraler Finanzbuchhaltungssoftware in Eigenregie gezwungen, die Prüfung im Bereich der Daten- und Programmsicherheit - zumindest in solchen Fällen - auszuweiten und zu vertiefen. Ein erhöhter Prüfungsaufwand und damit auch höhere Prüfungsgebühren bei der jeweiligen Kommune sind die zwangsläufige Folge.

Die notwendigen Prüfungshandlungen verursachen insoweit ggf. einen zusätzlichen Aufwand für die örtliche Prüfung bzw. bei jeder einzelnen Kommune einen zusätzlichen Aufwand im Rahmen der überörtlichen Prüfung.

4 Fazit

Der Einsatz autonomer Finanzsoftware, anstelle der vom DV-Verbund angebotenen Verfahren, führt zu einer unmittelbaren Zunahme der Risikoverantwortung der Kommune. Damit die Kommune dieser Verantwortung gerecht wird, muss sie entsprechende Maßnahmen veranlassen bzw. Aufgaben wahrnehmen, die zu direktem eigenem monetären Aufwand führen (zusätzliches Personal, bauliche, sicherheitstechnische Maßnahmen usw.).

Weiterer monetärer Aufwand kommt durch die Inanspruchnahme Dritter hinzu (z. B. Prüfungsgebühren im Rahmen der überörtlichen Anwendungsprüfung bzw. der Programmprüfung). Soweit z. B. Mängel im Rahmen der Anwendungsprüfung festgestellt werden, wird deren Beseitigung ebenfalls regelmäßig zu weiteren Kosten bei der Kommune führen (z. B. zusätzliche Maßnahmen zur notwendigen Erhöhung des Sicherheitsniveaus).