EINGEGANGEN
12. OKT. 2023

gpa
Gemeindeprüfungsanstalt
Baden-Württemberg

Gemeindeprüfungsanstalt BW · Hoffstr. 1a · 76133 Karlsruhe

Komm.ONE AöR
Krailenshaldenstr. 44
70469 Stuttgart

Bearbeiter: Anja Womann
Telefon: 0721 / 8 50 05 – 170
Telefax: 0721 / 8 50 05 – 370
Anja.Womann@gpabw.de

Aktenzeichen: 094088
Unser Schreiben v.:
Ihr Zeichen:
Ihr Schreiben v.: 10.08.2023

Karlsruhe, 10.10.2023

Prüfung des ADV-Verfahrens „Digitale Signatur - medienbruchfreie Anordnung“ nach § 114a GemO
Abschließender Prüfungsvermerk - Testat

Sehr geehrte Damen und Herren,

die GPA hat das von der Komm.ONE AöR angebotene und von der Fa. Dataplan Computer Consulting GmbH entwickelte Anordnungs-Workflow-Verfahren **"Digitale Signatur - medienbruchfreie Anordnung"** (nachfolgend „Digitale Signatur“) in der Version 3.0.2016 und 3.0.2020 gemäß § 114a GemO geprüft. Über die Prüfung wurde am 30.03.2023 ein Bericht erstellt. Die Komm.ONE hat zum Prüfungsbericht mit Schreiben vom 10.08.2023 Stellung genommen.

1 Ergebnis der Prüfung

Die Prüfungsfeststellungen sind nach der Stellungnahme erledigt oder können aufgrund der bisher veranlassten Maßnahmen als erledigt gelten.

Bei den nachfolgenden Randnummern handelt es sich um ergänzende Empfehlungen bzw. Hinweise für die Programmanwendung.

Rdnr.	Ergänzende Empfehlungen bzw. Hinweise für die Programmanwendung

Passwortverwaltung

4 Im ADV-Verfahren ist eine umfangreiche Passwortverwaltung integriert. Damit können beispielsweise die Anzahl der Anmeldeversuche festgelegt und Passworte hinsichtlich ihrer Mindestlänge und Komplexität definiert werden. Es liegt in der Verantwortung des Anwenders, die Verfahrensfunktionen der Passwortverwaltung für die Programm- und Datensicherheit zu nutzen. Auf die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) wird hingewiesen.

Unterstützung der Trennung der Verantwortungsbereiche

5 Im ADV-Verfahren „Digitale Signatur" kann der kassenrechtliche Anordnungsprozess für Einnahmen und Ausgaben mit einer sonstigen elektronische Signatur nach § 28 Abs. 3 GemKVO abgewickelt werden.

Es lassen sich mehrere sog. Postkörbe einrichten; die Einrichtung zumindest eines Postkorbs (entspricht einem Genehmigungsschritt im Anordnungsworkflow) ist unabdingbar durch das Verfahren vorgesehen. Die Einrichtung erfolgt in der Regel zusammen mit der Fa. Dataplan Computer Consulting GmbH.

Einige Anwender benötigen nur einen Postkorb (Prozessschritt), da bereits auf der eingehenden Papierrechnung ein Stempel mit dem Vermerk "sachlich/rechnerisch richtig und Datum / Unterschrift" angebracht wird (nachfolgend „Stempelverfahren") und anschließend die Rechnung mit der bereits erfolgten Feststellung der sachlich und rechnerischen Richtigkeit eingescannt wird.

Optional können mehrere Postkörbe als Genehmigungsschritte im elektronischen Workflow eingerichtet werden, beispielsweise für die Feststellung der „sachlichen und rechnerischen Richtigkeit" oder für die Vorgabe bestimmter sonstiger „Genehmigungsschritte" in Abhängigkeit einer bestimmter Betragsgrenze (z.B. für Zwecke der Visaprüfung durch das Rechnungsprüfungsamt).

Dabei können die „systemnahen" Tätigkeiten bzgl. der Verwaltung des Postkorbs (Aktivgrenzen, Notwendigkeit neuer Zeichner und des Postkorbs, Zeichner, Parameter, Ebenen, Routen) gesondert geschützt werden.

Die Verfahrensabläufe sind durch Vorkehrungen des Verfahrens (z.B. Passwortschutz, Protokollierung, usw.) ausreichend gesichert, so dass bei entsprechender Anwendung

ein höheres Maß an Sicherheit als bei dem papiergebundenen Anordnungsprozess gegeben ist.

Es liegt im Verantwortungsbereich des Anwenders, die vom ADV-Verfahren angebotenen Möglichkeiten entsprechend zu nutzen. Die Berechtigungen zur Verwaltung des Postkorbs sollten wegen der weitreichenden Auswirkungen restriktiv vergeben werden. Sie können zur besseren Trennung der Verantwortungsbereiche analog der Benutzerverwaltung an eine gesonderte Stelle (z.B. IuK-Abteilung) ausgelagert werden.

Abbildung der Funktionstrennung

6 Soweit nur ein Postkorb vorhanden ist (s. Rdnr. 5), ist organisatorisch sicherzustellen, dass eine Trennung von (manueller) Feststellung und (elektronischer) Anordnung erfolgt.

Werden mehrere Postkörbe im ADV-Verfahren eingerichtet, ist die automatisierte Sicherstellung der Trennung der Verantwortungsbereiche durch das Verfahren technisch möglich. Allerdings kann der Zugriff auf die Postkörbe demselben Benutzer zugeordnet und insoweit die programmtechnisch vorgesehene Funktionstrennung unterlaufen werden.

Soweit Rechnungen bereits in elektronischer Form eingehen, sollte ein (zumindest) zweistufiges Genehmigungsverfahren mit der Trennung von Feststellung und Anordnung implementiert werden, da anderenfalls ein unnötiger Medienbruch (Ausdruck der elektronischen Rechnung, Abstempeln und Rechnungsscan) herbeigeführt werden müsste, welcher aufwändig und fehleranfällig wäre.

Dem Anwender obliegt die Verantwortung für geregelte und sichere Abläufe unter Einhaltung der kassenrechtlichen Funktionstrennung. Er hat vor Ort die erforderlichen organisatorische Maßnahmen zu ergreifen. Auf die besondere Bedeutung eines internen Kontrollsystems wird hingewiesen.

Elektronischer Sichtvermerk

9 Neben dem „Stempelverfahren“ (s. Rdnr. 5) bietet das Verfahren die Möglichkeit, einen Sichtvermerk elektronisch an der eingescannten Rechnung anzubringen. Im Ausnahmefall, wenn kein dezentraler Verfahrenszugriff in Fachbereichen (Fachabteilungen), sondern lediglich ein zentraler Zugriff auf das Verfahren erfolgt, nutzen Anwender, die nur einen Postkorb eingerichtet haben, diesen Sichtvermerk für Zwecke der sachlichen und rechnerischen Feststellung (ggf. mit ergänzenden Anmerkungen).

Während des Programmprüfungsverfahrens wurde die Mitgabe eines einheitlichen Zusatztextes zur eindeutigen Kennzeichnung des elektronischen Sichtvermerks für eine Feststellung der sachlichen und rechnerischen Richtigkeit implementiert. Darüber hinaus können fehlerhafte Vorgänge ohne Unterzeichnung abgewiesen werden. Der elektronische Sichtvermerk zur Feststellung der sachlichen und rechnerischen Richtigkeit wird als Dokument gespeichert und ist fest mit der Anordnung verbunden. Das Sichtvermerks-Dokument kann vom fachlich Sachbearbeitenden (Standardanwender) nicht mehr gelöscht werden. Lediglich Benutzer mit der Berechtigung eines Postkorbverwalters haben das Recht, diese Dokumente im Ausnahmefall („Notfalleingriff") zu löschen.

Die Nutzung des elektronischen Sichtvermerks sollte allerdings Ausnahmefällen vorbehalten bleiben, da die Prüfung, ob in jedem Fall eine Feststellung der sachlichen und rechnerischen Richtigkeit erfolgte, aufwändiger ist und der Prozess-Schritt umgangen werden kann. Es obliegt dem Anwenden in eigener Verantwortung, eine entsprechende Absicherung durch das interne Kontrollsystem sicherzustellen.

Festsetzungen in Fachanwendungen – sachliche und rechnerische Richtigkeit

10 Mit dem Verfahren können auch Veranlagungsdaten aus Fachverfahren (z.B. Grund- und Gewerbesteuer) weiterverarbeitet werden. Je nach Art des automatisierten Anordnungs- und Feststellungsverfahren kann anstelle der Feststellung nach § 11 Abs. 1 GemKVO (Einzelbescheinigung) auch eine Bescheinigung nach § 11 Abs. 4 GemKVO (Teilfeststellungsbescheinigung) erfolgen. In diesen Fällen erfolgt die sachliche und rechnerische Feststellung außerhalb des Verfahrens.

Die buchungsrelevanten Prozess-Schritte sind vom Anwender für seine vor Ort bestehende Organisation des Arbeitsablaufs zu definieren (beispielsweise auch, mit welcher Funktion in welchem Verfahren welcher kassenrechtliche Prozess-Schritt erfolgt). Eine Feststellung der sachlichen und rechnerischen Richtigkeit im ADV-Verfahren „Digitale Signatur – Medienbruchfreie Anordnung" durch einen eigens hierfür eingerichteten Postkorb ist nicht notwendig, soweit diese bereits anderweitig, z.B. beim vorgelagerten Fachverfahren, erfolgte.

Verfügbarkeitskontrolle

11 In der Erfassungsmaske des Rechnungseingangsbuches (REB) ist das Eingabefeld „Verfügbar" für die Abbildung der Verfügbarkeitskontrolle enthalten. Das Feld ist mit dem Planungsmodul, in dem die verfügbaren Mittel erfasst werden, verbunden. Eine Mittelüberschreitung hat programmtechnisch zunächst keine Auswirkungen. Denkbar wäre al-

lerdings, einen weiteren Postkorb zu erstellen, der (nur) dann angesteuert wird (manuelle Auswahl per Checkbox nach Sichtkontrolle durch den Anwender), wenn keine verfügbaren Mittel vorhanden sind.

Zahlungsanordnungen müssen bei über- oder außerplanmäßigen Ausgaben die Bestätigung des Bewirtschaftungsbefugten über das Vorliegen der Voraussetzungen für derartige Ausgaben enthalten (§ 8 Abs. 1 Nr. 6 GemKVO).

Der Anwender wird bei Budget-Überschreitungen durch eine Warnmeldung auf den Sachverhalt hingewiesen. Die Anlage eines (optionalen) Postkorbs zur Mittelprüfung wird empfohlen. Anderenfalls muss der Anwender auf andere Weise das Vorliegen der haushaltsrechtlichen Voraussetzungen für die außer-/überplanmäßigen Ausgaben außerhalb des Verfahrens dokumentieren.

Programmprüfung und Programmfreigabe

14 Die Programmprüfung und die Freigabe des Programms sind selbständige Entscheidungen mit unterschiedlichen Zuständigkeiten. Die Kommune darf nur solche Programme einsetzen, die vom Bürgermeister oder einer von ihm bestimmten Stelle nach Sicherstellung der in § 6 GemKVO i.V. mit § 35 Abs. 5 und 6 GemHVO genannten Voraussetzungen freigegeben worden sind.

Im Übrigen ersetzt die Programmprüfung nicht die Programmfreigabe und eine erfolgte Programmfreigabe nicht die Programmprüfung nach § 114a GemO. Die freigebende Stelle bei der Kommune kann sich aber bei der Programmfreigabe auf die Erkenntnisse der Programmprüfung stützen.

Customizing

15 Das ADV-Verfahren kann durch eine Vielzahl von Einstellungen individuell konfiguriert werden. Wegen der damit verbundenen Auswirkungen auf die Ordnungsmäßigkeit der Programme wird auf die GPA-Mitteilung 2/2000 verwiesen.

Sichtkontrolle des Scanprodukts

16 In Papierform eingehende Rechnungen werden beim Anwender am Scanarbeitsplatz gescannt, nach Geschäftsdaten (kassenrechtlichen Anordnungsinhalten) automatisiert durchsucht und die gefundenen Anordnungsinhalte in den FINANZ+-Datenfeldern sowie die Rechnung als Wiedergabe des Papieroriginals im PDF-Format im angeschlossenen Dokumentenmanagement-System (DMS/Archivsystem) gespeichert.

Es ist hierbei sicherzustellen, dass die (in den papiergebundenen Original-Rechnungen) gespeicherten Daten nicht verloren gehen oder unbefugt (unbeabsichtigt) geändert werden (§ 6 GemKVO i.V.m. § 35 Abs. 5 Satz 2 Nr. 3 GemHVO). Die Unterlagen müssen bis zum Ablauf der Aufbewahrungsfrist verfügbar und jederzeit in angemessener Frist lesbar gemacht werden können (§ 6 GemKVO i.V.m. § 35 Abs. 5 Satz 2. Nr. 5 und § 39 Abs. 2 GemHVO). Die Verarbeitungsfähigkeit muss, angefangen von der maschinellen Erfassung über die weiteren Bearbeitungsstufen, sichergestellt sein. Durch Kontrollen ist sicherzustellen, dass alle Geschäftsvorfälle vollständig erfasst werden (§ 6 GemKVO i.V.m. § 35 Abs. 5 Satz 1 GemHVO und Ziff. 3.1 GoBS). Dies bedingt, dass alle gescannten Rechnungen mit dem Original abgeglichen und etwaige Abweichungen oder Lücken bei der Erfassung korrigiert werden, so dass eine Übereinstimmung von Daten (sowohl in den Datenfeldern als auch bei den Bilddaten im DMS) mit dem Original erreicht wird. Dies bedingt auch, dass ausschließlich die Rechnungen und nicht etwa Lieferscheine, Angebote, Rechnungsduplikate oder sonstige Schriftstücke mit Geschäfts- oder Rechnungsdaten wie fremde Barcodes, usw. fälschlicherweise als Vorgang erfasst werden. Außerdem müssen Detailänderungen, z.B. neue Kontonummer bei sonst gleichbleibenden Lieferanten-Daten, bemerkt, erfasst und berücksichtigt werden.

Der Sichtkontrolle des Scanprodukts kommt eine entscheidende Bedeutung im Gesamtprozess zu. Auf die Veröffentlichungen des BSI wie beispielsweise die „TR03138 Ersetzendes Scannen“ (RESISCAN) und „Ersetzendes Scannen leichtgemacht – eine Handlungshilfe für Institutionen und Unternehmen“ sowie den Praxisleitfaden der KGSt „Ersetzendes Scannen“ (KGSt-Bericht Nr. 8/2017) in der jeweils aktuellen Version wird verwiesen.

Im Rahmen des Internen Kontrollsystems ist der Sichtkontrolle beim Scanvorgang eine besondere Bedeutung beizumessen.

2 Rahmen- bzw. Einsatzbedingungen der Prüfung

Das ADV-Verfahren ist innerhalb der Systemanbindung an das ADV-Verfahren FINANZ+ - Kommunale Doppik der Fa. Dataplan Computer Consulting GmbH und auf Grundlage der bei der Gemeinde Urbach verwendeten Systemeinstellungen geprüft worden.

Bereich/Funktion	Wesentliche Einsatzbedingungen	M[1]
Postkörbe allgemein	Ein Postkorb bildet einen Genehmigungsschritt im Anordnungsworkflow ab. Zumindest ein Postkorb für die Fertigung der kassenrechtlichen Anordnung muss vorhanden sein.	S
Bei Anlage nur eines Postkorbs	Die Bestätigung der sachlichen und rechnerischen Richtigkeit muss außerhalb des Verfahrens (manuell) erfolgen; der Postkorb im Verfahren dient der Fertigung der kassenrechtlichen Anordnung.	S
Weitere Postkörbe	Weitere Postkörbe für die Feststellung der sachlichen und rechnerischen Richtigkeit oder beispielsweise für die Visaprüfung durch ein Rechnungsprüfungsamt können implementiert werden.	I

Das Ergebnis der Programmprüfung bezieht sich auf diese Einsatzbedingungen.

3 Geprüfte Bereiche

Im Wesentlichen sind die folgenden zentralen Finanzvorgänge (sog. Kernprozesse) geprüft worden:

- Ersatz der handschriftlichen Unterschrift bei der (sachlichen und rechnerischen) Feststellung nach § 11 GemKVO durch die sonstige elektronische Signatur nach § 28 Abs. 3 GemKVO und die verwendete Protokoll-Lösung.
- Ersatz der handschriftlichen Unterschrift des Anordnungsberechtigten nach § 8 Abs. 1 Nr. 9 GemKVO durch die sonstige elektronische Signatur nach § 28 Abs. 3 GemKVO und die verwendete Protokoll-Lösung.
- Zugriff (aus dem Anordnungsworkflow heraus) auf die revisionssicher archivierten signierten Anordnungen und die weiteren Belege.
- Integration in die Systemumgebung (Integrität des Geschäftsprozesses).

[1] Merkmal: S = im Rahmen der Prüfung als Standard angesehene Rahmenbedingung des Programmeinsatzes; Merkmal: I = individuelle Einsatzbedingung (Projektarbeit Anwender).

Dabei wurden insbesondere folgende Kriterien mitberücksichtigt:

- Angemessenheit der Programmdokumentation.
- Ordnungsmäßigkeit der Verarbeitung der Daten.
    - Hinreichende Implementierung von maschinellen Erfassungskontrollen (Plausibilitätsprüfungen).
    - Vollständigkeit und Richtigkeit der zentralen Verarbeitungsprozesse einschließlich der Systemausgaben (z.B. Listen und Auswertungen mit Beleg- oder Buchfunktion).
    - Gewährleistung der Nachvollziehbarkeit der Geschäftsvorfälle.
- Schutzmechanismen des ADV-Verfahrens gegen Verlust und unberechtigte Änderungen von Daten.
    - Protokollierungsfunktion, bezogen auf die Protokollierung des Zeichnungsvorgangs.
    - Passwortverwaltung.
    - Grundsystematik der Berechtigungsverwaltung, bezogen auf die Berechtigungen bei der elektronischen Signatur im Anordnungs-Workflow:
        - Verfahrenstechnische Unterstützung der Trennung von Verantwortungsbereichen (insbesondere Trennung von Anordnung, Vollzug und Administration) durch entsprechende Zugriffsmechanismen.
        - Möglichkeit der Trennung von ändernden und lesenden Berechtigungen usw.
        - Systemreaktionen bei unberechtigten Zugriffen.
        - Nachvollziehbarkeit der Benutzer- und Berechtigungsverwaltung (Revisionssicherheit).

4 Nicht geprüfte Bereiche

Nicht geprüft worden sind folgende Bereiche:

- Die eingesetzte Scanhardware und die dabei verwendete Scansoftware (hierzu kann u.a. auf die Anforderungen aus der Technischen Richtlinie 03138 „Ersetzendes Scannen (RESISCAN)" des Bundesamts für die Sicherheit in der Informationstechnik und den Bericht der KGSt®-Nr. 8/2017 „Ersetzendes Scannen, Praxisleitfaden für Kommunen" verwiesen werden).

- Empfang und technische Übergabe von „E-Rechnungen".

- Der Prozessschritt der (manuellen) Validierung von gescannten, empfangenen oder manuell eingetragenen Rechnungen und dem Löschen von Fremdbelegen vor Initiieren des kassenrechtlichen Workflowprozesses.

- Systembestandteile und Systemfunktionen, die direkt den FINANZ+-Standard verwenden bzw. darauf zugreifen, z.B. Passwortverwaltung, Freigabe von Daueranordnungen, Verfügbarkeitskontrolle usw.

- Der direkte Zugriff auf das Archivierungsverfahren bzw. dessen Programmbestandteile. Die Prüfung der revisionssicheren Archivierung erfolgte vielmehr geschäftsprozessbezogen aus dem Workflow heraus.

- Geschäftsjahreswechsel.

- Funktionen, die vom Hersteller oder Anbieter zur Anwendung ausdrücklich nicht empfohlen werden. Hier ist es insbesondere Aufgabe der für die Programmfreigabe zuständigen Stelle, im Freigabevermerk diese Funktionen auszunehmen und durch technische bzw. organisatorische Maßnahmen deren Einsatz zu unterbinden.

- Reports/Listen bzw. sonstige Auswertungen, soweit sie zur Einhaltung der Ordnungsmäßigkeit nicht erforderlich sind (z.B. Listen ohne Beleg- und Buchfunktion, die individuell vom Anwender erstellt werden können); statistische Auswertungen.

- Extraktion von Daten aus dem Bestand; Down- und Uploadfunktionen.

- Tools und Funktionen, die zum einmaligen Einsatz, z.B. für Releasewechsel, für Konvertierungen, bei der Implementierung oder zur Migration vorgesehen sind (z.B. Altdatenübernahme); Tools zur Optimierung des Drucklayouts; Funktionen zur Datenarchivierung, Möglichkeiten zur flexiblen Erweiterung von Verfahrensinhalten um anwenderspezifische Felder.

- (Individuelle) Umsetzung einer ordnungsgemäßen Benutzer- und Berechtigungsverwaltung sowie des ordnungsmäßigen DV-Betriebs beim Anwender.
    - Ausgestaltung (Ausprägung) der Berechtigungen (z.B. in der Form von Berechtigungsrollen).
    - Zuordnung der Berechtigungen zu den jeweiligen Usern (Sachbearbeitern) auf Grundlage der individuellen organisatorischen Rahmenbedingungen beim Anwender.
    - Nutzung der vom ADV-Verfahren angebotenen Möglichkeiten bei der Passwortvergabe (Mindestlänge, Sperrung des Zugangs nach einer bestimmten Anzahl von Fehlversuchen usw.).
    - Aktivierung der Protokollierungsfunktion.
    - Eingriffsmöglichkeiten des Anwenders mittels eigener Zusatzprogramme bzw. -tools (z.B. auf Datenbank- oder Betriebssystemebene).

5 Abschluss der Prüfung

Zum Abschluss der Prüfung nach § 114a GemO wird das nachfolgende Testat ausgestellt. Der Ablauf, Inhalt, Umfang und das Ergebnis der Prüfung, die der Prüfung zugrunde gelegten Einsatzbedingungen und die Art und Weise der Erledigung der Prüfungsfeststellungen sind im Prüfungsbericht vom 30.03.2023 und den sich anschließenden weiteren Unterlagen dokumentiert. Die genannten Unterlagen bilden die Grundlage dieses Prüfungsvermerks.

Mit freundlichen Grüßen

gez. Stefan Ulmer

Anlage
Testat