Amt Stralendorf
DER AMTSVORSTEHER

Amt Stralendorf für:
- die Gemeinde Dümmer
- die Gemeinde Holthusen
- die Gemeinde Klein Rogahn
- die Gemeinde Pampow
- die Gemeinde Schossin
- die Gemeinde Stralendorf
- die Gemeinde Warsow
- die Gemeinde Wittenförden
- die Gemeinde Zülow

• Amt Stralendorf • Amtsverwaltung • Dorfstr. 30 • 19073 Stralendorf •

Landkreis Ludwigslust-Parchim
Der Landrat
Persönlich Frau Ziegert
Putlitzer Str. 25
19370 Parchim

Telefon 03869 / 7600-0
Telefax 03869 / 7600-60
E-Mail: amt@amt-stralendorf.de

Fachdienst II – Finanzen
Liegenschaften
Ihr Bearbeiter:
Herr Borgwardt
Telefon 03869/ 760012
e-mail. borgwardt@amt-stralendorf.de

Ihre Zeichen:	Ihre Nachricht vom:	Unser Aktenzeichen:	Unsere Nachricht vom:	Datum
		Bo/RPA2015-2018-IKS-Amt		2022-09-20

Stellungnahme zum Bericht des Rechnungsprüfungsamtes des Landkreises LuP zur überörtlichen Prüfung des Amtes Stralendorf und dem dazu erfolgten Auswertungsgespräch für die Jahre 2015 bis 2018 für die Prüfungsschwerpunkte IKS, Finanzanwendung und IT

Sehr geehrte Frau Ziegert,

Zu den einzelnen Punkten möchte ich wie folgt Stellung nehmen:

P1	Die Amtsverwaltung ist ab dem 01.01.2020 der KSM als Träger beigetreten, sodass die Aufgaben der Betreuung der IT-Landschaft im Amt Stralendorf auf die KSM vollständig übertragen wurde. Hierdurch ist eine Stelle für die Systemadministration nicht mehr zwingend vorzuhalten. Eine neue Stelle für den Bereich Digitalisierung wurde installiert und wird die Koordination der IT-Dienstleitung und des Datenschutzes übernehmen.
P2	Die entsprechenden Verträge liegen nunmehr vor.
P3	Die Aufgabe des behördlichen Datenschutzbeauftragten wurde ab dem 01.01.2021 ebenfalls auf die KSM übertragen, sodass die entsprechenden Bestellungsurkunden vorliegen. Weiterhin wurde die Bestellungsurkunde vom 19.11.2002 aufgehoben.

P4	Mit Übertragung des behördlichen Datenschutzes an die KSM konnten neue Strukturen im Bereich Datenschutz installiert werden und werden regelmäßig auf Aktualität überprüft. Weiterhin erfolgen regelmäßige Schulungen der Beschäftigten, sowie Begehungen durch den Datenschutzbeauftragten.
P5	Die Beschäftigten wurden ausdrücklich auf die Einhaltung der Regelungen zum Datenschutz, der DA Nr. 3 und der Vertraulichkeit hingewiesen und die Einhaltung wird durch die Fachdienstleitungen überprüft.
P6	Eine Anpassung der Dienstanweisung erfolgt zeitnah.
P7	Ein Benutzerkonzept für alle Fachanwendungen wird zeitnah erarbeitet.
P8	Im Zuge der Migration wurden die Passwortrichtlinien der KSM übernommen und kommen entsprechend zur Anwendung.
P9	Diese Aufgabe wurde im Zuge der Trägerschaft der KSM übertragen.
P10	Mit Einrichtung des neuen Serverraums durch die KSM wurde der Mängel abgestellt.
P11	Die Verfahrensdokumentation für das Rechnungswesen H&H pro Doppik wird zeitnah umfangreich aufgearbeitet.
P12	Durch die Migration zur KSM wurde die Technik auf den neusten Stand gebracht und erforderliche Updates durchgeführt, um die Sicherheitslücken zu schließen.
P13	Zwischenzeitlich wurde die letzte Änderung des Fachverfahrens HKR im Jahre 2020 freigegeben. Seit Dezember 2020 ist das Amt mit seinen Fachverfahren in der Cloud der AöR KSM, welche die zukünftige Freigabe übernommen hat.
P14	Der Prüfvermerk wird zur Kenntnis genommen und für zukünftige Versionswechsel etc. berücksichtigt.
P15	Die entsprechenden Unterlagen wurden bereits mit unserem Datenschutzbeauftragten erarbeitet und liegen somit vor.
P16	Die Datenschutz-Folgenabschätzung ist seitens unseres Datenschutzbeauftragten in der Erarbeitung und liegt zeitnah vor.
P17	Wird zukünftig direkt von der KSM verwaltet und in Abstimmung mit dem Amt laufend aktualisiert.
P18	Der Prüfvermerk wird zur Kenntnis genommen und entsprechend zur Umsetzung herangezogen.
P19	Die Finanzdienstanweisung soll bis Ende 2022 überarbeitet werden.
P20	Die DA zur Organisation des Rechnungswesens wird zukünftig geändert.
P21	Wird zukünftig beachtet.

Für die Hinweise zur Beseitigung der Mängel Ihrerseits und von Seiten der Mitarbeiter und Mitarbeiterinnen des Bereiches Rechnungsprüfung möchte ich mich herzlich bedanken.

Mit freundlichen Grüßen

Richter
Amtsvorsteher

LANDKREIS
LUDWIGSLUST-PARCHIM
RAUM FÜR ZUKUNFT

Der Landrat
des Landkreises Ludwigslust-Parchim
als Gemeindeprüfungsamt

Teilbericht mit den Prüfungsschwerpunkten IKS, Finanzanwendung und IT im Amt Stralendorf

Ansprechpartner: Manuela Golnik
Telefon: 03871 722 1417
Telefax: 03871 72277 1417
E-Mail: manuela.golnik@kreis-lup.de

Landkreis Ludwigslust-Parchim
Putlitzer Straße 25
19370 Parchim
www.kreis-lup.de

Postadresse:
Postfach 1263
19362 Parchim

Inhaltsverzeichnis

Grundsätzlich verwendet das Gemeindeprüfungsamt des Landkreises Ludwiglust-Parchim im Bericht geschlechtsneutrale Begriffe. Werden Personenbezeichnungen aus Gründen der besseren Lesbarkeit lediglich in der männlichen oder weiblichen Form verwendet, so schließt dies das jeweils andere Geschlecht mit ein.

Abkürzungsverzeichnis

AöR	Anstalt des öffentlichen Rechts
Art.	Artikel
AV	Auftragsverarbeitung
BfDI	Bundesbeauftragter für den Datenschutz
BSI	Bundesamtes für Sicherheit in der Informationstechnik
DA	Dienstanweisung
DFÜ	Datenfernübertragung
DSB	Datenschutzbeauftragter
DV	Datenverarbeitung
EDV	Elektronische Datenverarbeitung
FD	Fachdienst
GDSB	Gemeinsamer Datenschutzbeauftragte
H	Hinweis
HHJ	Haushaltsjahre
IKS	Internes Kontrollsystem
IS	Informationssicherheit
IT-DL	IT-Dienstleister
LVB	Leitender Verwaltungsbeamte
Pkt.	Punkt
S	Satz
SB	Sachbearbeiter
V	Version
VV	Verwaltungsvorschrift
ZV eGo-MV	Zweckverband Elektronische Verwaltung in M-V

Beispiele:

GV-Sitzung, HH-Führung, RP-Amt, RP-Ausschuss

Rechtsgrundlagen

DSG M-V	Datenschutzgesetz Mecklenburg-Vorpommern
DS-GVO	EU Datenschutz – Grundverordnung
EGovG M-V	Gesetz zur Förderung der elektronischen Verwaltungstätigkeit in Mecklenburg-Vorpommern
EVB-IT	Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen
GemHVO-Doppik M-V	Gemeindehaushaltsverordnung-Doppik
GemHVO-GemKVO-DoppVV M-V	Verwaltungsvorschrift zur Gemeindehaushaltsverordnung-Doppik und Gemeindekassenverordnung-Doppik des Innenministeriums
GemKVO-Doppik M-V	Gemeindekassenverordnung-Doppik
GoB	Grundsätze ordnungsmäßiger Buchführung
GoBD	Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
KPG M-V	Kommunalprüfungsgesetz Mecklenburg-Vorpommern
KV-MV	Kommunalverfassung für das Land Mecklenburg-Vorpommern
NKHR M-V	Neues kommunales Haushalts- und Rechnungswesen Mecklenburg-Vorpommern
PersVG M-V	Personalvertretungsgesetz M-V

Bei der Prüfung wurde der auf die geprüften HHJ zutreffende Rechtsstand berücksichtigt.

Glossar

Active Directory	Active Directory Domain Service (ADDS). Mit ADDS kann man ein Netzwerk der Struktur einer Organisation oder seiner räumlichen Verteilung nachbilden. Dazu speichert und verwaltet Active Directory Informationen über Netzwerk-Objekte und -Ressourcen. Netzwerk-Ressourcen sind Zugriffsberechtigungen, Nutzungsrechte für Anwendungen, Speicherplatz, Netzwerkdienste und Netzwerk-Peripherie (Drucker, Computer).
Administration	Verwaltung eines IT-Systems
Aktive Komponenten	Kernstück eines IT-Netzwerkes. Geräte mit denen man über Signale Daten in einem Netzwerk oder weitere IT-Netzwerke verbinden kann
Anwendung	Anwendungssoftware
Archiv(system)	dient der langfristigen und unveränderlichen Speicherung von aufbewahrungspflichtigen Daten und Unterlagen auf maschinenlesbaren Datenträgern zur Umsetzung der gesetzlichen Aufbewahrungsfristen
Aufbewahrungsfrist	Zeitraum, in dem Unterlagen aufgrund gesetzlicher Vorgaben aufbewahrt werden müssen
Authentizität	tatsächliche Identität. Ein System prüft die Anmeldeinformationen eines Benutzers
automatisierte Verfahren	Auf der Basis von gleichartigen elektronischen Verarbeitungsprozessen kann eine große Menge von Informationen nach bestimmten Merkmalen elektronisch erfasst, zugänglich und ausgewertet werden
Benutzer	ist die festgelegte identifizierbare Bezeichnung für eine Person in einem IT-Netzwerk.
Benutzergruppe, Gruppenkonten	Benutzerkonten, denen gleiche Zugriffsrechte zugeordnet wurden.
Benutzerkonto	ist eine Zugangsberechtigung zu einem zugangsbeschränkten IT-System
Client	bezeichnet ein Computerprogramm, das auf dem Endgerät eines Netzwerks ausgeführt wird und mit einem Server kommuniziert
Datenbank	Ist ein elektronisches Verwaltungssystem, das besonders große Datenmengen abbilden kann.
Datenschutz	Unter Datenschutz versteht man den Schutz personenbezogener Daten vor dem Missbrauch durch Dritte (nicht zu verwechseln mit Datensicherheit)[1]
Datensicherheit	Mit Datensicherheit wird der Schutz von Daten hinsichtlich gegebener Anforderungen an deren Vertraulichkeit, Verfügbarkeit und Integrität bezeichnet. Ein anderer Begriff dafür ist „Informationssicherheit"[2]

[1] Leitfaden Informationssicherheit, Bundesamt für Sicherheit in der Informationstechnik –BSI, Begriffe rund um die Informationssicherheit

[2] Leitfaden Informationssicherheit, Bundesamt für Sicherheit in der Informationstechnik –BSI, Begriffe rund um die Informationssicherheit

Digital	Prozesse, Dokumente sind nur mit einem IT-System einsehbar bzw. nutzbar
Dokumente	umfasst Träger von Informationen auf Papier aber auch IT-gestützte erzeugte Objekte
EBICS	Electronic Banking Internet Communication Standard, standardisiertes Sicherungs- und Übertragungsstandard über das Internet zwischen Kunde und Bank
Elektronische Signatur	Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und zur Authentifizierung dienen
E-Mail	elektronische Post
Fernwartung	erbrachte IT-Dienstleistungen ohne örtliche Präsenz
H&H proDoppik	Kommunales Finanzmanagement
Implementierung, Schnittstelle	Transfer von Daten in eine andere Umgebung ohne inhaltliche Veränderung der Informationen
ISMS	Managementsystem für Informationssicherheit. Innerhalb eines ISMS sind Regeln, Verfahren und Maßnahmen zu definieren, mit denen sich die Informationssicherheit in einer Organisation steuern, kontrollieren und sicherstellen lässt. Alle zu schützenden Daten sind gleich zu behandeln. Ein ISMS ersetzt daher kein Datenschutz-Managementsystem. Das Aufstellen eines ISMS liegt im Verantwortungsbereich einer Organisationsleitung.
ISO 2700x	Ist eine internationale Norm für Informationssicherheit in privaten, öffentlichen oder gemeinnützigen Organisationen. Die Normenfamilie beschreibt die Anforderungen zur Implementierung eines ISMS u. a. in Bezug auf Integrität, Verfügbarkeit und Vertraulichkeit.
IT	Informations- und Datenverarbeitung auf der Basis technischer und softwareseitiger Infrastrukturen
LAN	Local Area Network, Computernetzwerk
Login-Name	Benutzername für die Anmeldung an einem EDV-System
Logischer Netzwerkplan	zeigt den Datenfluss zwischen den Endgeräten in einem IT-Netzwerk
MS Office	bezeichnet Bürosoftware - Pakete von Microsoft für Windows
OKKSA	offener Katalog für kommunale Softwareanforderungen
Progress	Datenbank der Finanzanwendung „H&H proDoppik"
Originär	grundlegend
Passive Netzwerktechnik	Netzwerktechnik, die in einer IT-Infrastruktur fest installiert ist (Steckdosen, Buchsen, Kabel)
Passwort	Kennwort zur Sicherstellung der Identität eines Benutzers im IT-System
Patch, Patchlevel	Version, Revisionsnummer
Personenbezogene Daten	definiert in Art. 4 Abs. 1 Nr. 1 DS-GVO, „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen ; als identifizierbar wird eine

	natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;"
Physisch	ist die Eigenschaft körperlich zu existieren
Physischer Netzwerkplan	zeigt die Kabelverbindungen eines IT-Netzwerkes
Rechnungswesen	Gesamtheit aller Elemente und finanzrelevanten Geschäftsprozesse einer Buchführung
Release, R	freigegebene Softwarewareversion
Schnittstelle	Datei zur Übertragung von Daten von einer Fachanwendung in eine andere Fachanwendung
Server	Zentralcomputer
Support, UserHelpDesk	Beratungstätigkeit, Vereinbarte Dienstleistungen im IT-Service
Updates	aktualisierte Softwareprogramme
Verschlüsselung	Umwandlung von Klartext in ein Geheimtext
Virtuell	ist die Eigenschaft einer Sache, nicht in der Form zu existieren
VPN	Virtual Private Network, Technologie mit der man von außen auf ein internes Unternehmensnetzwerk zugreifen kann
Integrität, Verfügbarkeit und Vertraulichkeit	Grundwerte der Informationssicherheit[3]
Integrität	Jegliche Veränderung an gespeicherten Daten, deren Entfernung oder Schädigung durch unbefugte Dritte ist auszuschließen. Personenbezogene Daten dürfen nur in einer Weise verarbeitet werden, die einen Schutz vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen gewährleistet.
Verfügbarkeit	Dem Benutzer stehen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung.
Vertraulichkeit	Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.

[3] Leitfaden Informationssicherheit, Bundesamt für Sicherheit in der Informationstechnik –BSI, Begriffe rund um die Informationssicherheit

1. Allgemeine Vorbemerkungen

1.1 Prüfungsauftrag

Gemäß § 7 Abs. 1 Nr. 1 und 3 KPG M-V ist die Haushalts- und Wirtschaftsführung, die sonstige Verwaltungstätigkeit sowie die Organisations- und Wirtschaftlichkeitsprüfung Gegenstand der überörtlichen Prüfung.

Grundlage der Prüfung ist der Prüfungsauftrag für die überörtliche Prüfung des Amtes Stralendorf vom 16.12.2019, Prüfungsschwerpunkt 1.2.2 „Datenschutz, Finanzanwendung und IT-Prüfung".

Verantwortlich für die Organisation und Durchführung der Gesamtprüfung war die Prüfgruppenleiterin Frau Vogtland. Mit der Vornahme der diesem Bericht zugrundeliegenden Teilprüfung wurde Frau Golnik betraut. Die Prüfung erfolgte in den Monaten März und Juni 2020.

1.2 Prüfungsvoraussetzungen

Die durch das Amt Stralendorf einzuleitenden Maßnahmen ergeben sich aus nachfolgenden Rechtsgrundlagen:

- KV M-V,
- DS-GVO,
- DSG M-V,
- GemHVO-Doppik M-V,
- GemKVO-Doppik M-V und
- GoB.

Gemäß § 26 Abs. 13 und § 28 Abs. 1 GemHVO-Doppik M-V ist eine DA zur Sicherung des Buchungsverfahrens zu erlassen. Neben den Anforderungen an die Software zur automatisierten DV gemäß § 26 Abs. 10 GemHVO-Doppik M-V i. V. m. § 12 Abs. 1 GemKVO-Doppik M-V sind in dieser DA organisatorische Festlegungen, die den GoB entsprechen, zu treffen. Die GoBD sehen vor, dass zum Nachweis der Ordnungsmäßigkeit einer DV-gestützten Buchführung u. a. ein IKS vorzuhalten ist. Weitere gesetzliche Vorgaben, die den Erfordernissen des § 12 Abs. 1 Nr. 1 bis 11 GemKVO-Doppik M-V entsprechen, sind anzuwenden. Darüber hinaus sind interne Regelungen nach § 28 Abs. 2 Nr. 2a) bis 2h) GemHVO-Doppik M-V zu den örtlichen Gegebenheiten, hier die Einhaltung der Sicherheitsstandards, näher zu bestimmen.

Damit die Verarbeitung von personenbezogenen Daten mit einem bestimmten automatisierten Verfahren begonnen oder ein wesentlich geändertes Verfahren weiterhin genutzt werden durfte, waren bis zum 24.05.2018 die Voraussetzungen gemäß der §§ 18 - 22 DSG M-V sicherzustellen. Seit dem 25.05.2018 sind die Voraussetzungen gemäß DS-GVO einzuhalten.

Für einen optimalen Prüfungsverlauf wurde mit dem Prüfungsauftrag eine Anforderungsliste an das Amt Stralendorf übergeben. Für die v.g. Prüfung wurden die Unterlagen lt. Anforderungsliste Nr. 1.1 - 1.2, 2.4 - 2.8, 5.1 - 5.3 und 6 angefordert.

1.3 Prüfungsplanung

Im Amt Stralendorf wurde zum 01.01.2012 die Doppik im kommunalen Haushalts- und Rechnungswesen eingeführt. Um eine ordnungsgemäße Prüfung durchzuführen, wurde die DA zur Sicherung des Rechnungswesens angefordert.

Nachfolgende DA wurde übergeben:

- Finanzdienstanweisung zur Organisation des Rechnungswesens vom 01.01.2012 in der Fassung vom 19.03.2014.
- Finanzdienstanweisung zur Organisation des Rechnungswesens vom 01.01.2015 in der Fassung vom 07.03.2016.
- Finanzdienstanweisung zur Organisation des Rechnungswesens vom 01.01.2018 in der Fassung vom 12.04.2018.

Lt. VV zu § 34 GemKVO-Doppik M-V „ist der Leitfaden zur Erstellung von DA zur Organisation des Rechnungswesens in der Anlage 4 zu beachten und entsprechend der örtlichen Organisation anzuwenden.".

P *Zum Zeitpunkt der Doppik-Einführung lag keine DA zur Organisation des Rechnungswesens für das Amt Stralendorf vor.*

Nachfolgende Prüfungsplanung wurde festgelegt:

- Prüfung der Ablauforganisation Rechnungseingang und Zahlungsabwicklung innerhalb der Finanzanwendung,
- Prüfung Einsatz des Elektronischen Zahlungsverkehrs,
- Prüfung von erfassten personenbezogenen Informationen innerhalb der Finanzanwendung sowie deren Schutz vor unberechtigten Zugriffen, Verwaltung der Personenkonten,
- Prüfung der Sicherung des Buchungsverfahrens mit Einführung der Doppik im Rechnungswesen sowie
- die IT zum Prüfungszeitpunkt.

Zur Überprüfung, Bewertung und Sicherstellung eines ordnungsgemäßen Einsatzes der im Rechnungswesen eingesetzten DV-Programme wurden interne Festlegungen, Dokumentationen und Verträge zur Prüfung herangezogen. Zugleich wurden Hintergründe erfragt und Empfehlungen abgegeben.

2. Organisation der IT

In der Amtsverwaltung Stralendorf erfolgt seit dem 01.03.2020 eine Soft- und Hardwareumstellung auf das Kommunalunternehmen KSM - Kommunalservice Mecklenburg AöR. Die Aufgabenübertragung wurde im öffentlich-rechtlichen Vertag vom 18.12.2019, § 4 Abs. 1 und 10, geregelt. Nach Aussage des LVB soll die strukturierte Überführung der IT-Systeme bis Ende 2020 vollzogen werden. Eine Projekt- bzw. Terminplanung lag nicht vor. Während des Prüfungszeitraumes waren demzufolge noch IT-Systeme in der Amtsverwaltung installiert, die durch den bisherigen IT-DL gewartet wurden. Die Fernwartung der EDV-Umgebung führte der IT-DL über eine gesicherte VPN-Verbindung durch.

2.1 Stelle SB für Informationsverarbeitung

Die Stelle „Systemadministrator" (die Bezeichnung wurde aus der Stellenbeschreibung November 2018 übernommen) ist lt. Verwaltungsstruktur vom 14.10.2019 im Bereich des LVB eingerichtet.

P 1 *Die Stelle für Informationsverarbeitung war während der Prüfung personell nicht besetzt.*

H Die rasante Entwicklung im IT-Bereich wirft heute nicht nur eine Vielzahl technischer, sondern auch rechtlicher Aspekte auf die Tagesordnung. Zahlreiche Rechtsvorschriften, wie die DS-GVO oder das EGovG M-V, die unmittelbare Handlungspflichten für

die Datensicherheit und die DV festlegen, sind zeitnah umzusetzen. Grundsätzlich liegt die Verantwortlichkeit für alle EDV-Agenden beim Leiter der Organisationseinheit. Die v.g. Stelle sollte den neuen Gegebenheiten angepasst und personell besetzt werden. Die strategische Stellung in der Verwaltungsstruktur des Amtes Stralendorf wurde vorgenommen.

2.2 Öffentlich rechtlicher Vertrag – Kommunaler IT-Dienstleister KSM-AöR

Im öffentlich-rechtlichen Vertrag zur Beteiligung des Amtes Stralendorf an die KSM AöR vom 18.12.2019 wurde unter § 4 Abs. 1 und 10 die Aufgabenübertragung der Amtsverwaltung geregelt. Nachfolgende Sachverhalte wurden lt. § 4 Abs. 1 erfasst:

a) Betrieb eines kommunalen Rechenzentrums,

b) Systembetreuung für zentrale IT-Verfahren und –Systeme inklusive IT-Sicherheit und IT-Sicherheitsbeauftragten,

c) Zentrale Beschaffung von Hard- und Software,

d) Koordinierung und zentrale Beschaffung von notwendigen externen IT-Dienstleistungen,

e) Anwenderbetreuung durch einen zentralen Unterstützungsdienst,

f) Anwenderbetreuung für die eingesetzten Fachverfahren,

g) Sicherstellung einer kontinuierlichen Verbesserung der IT-Unterstützung und Planung von IT-Projekten,

h) Projektleitung und Projektbearbeitung im Rahmen der übertragenen Aufgaben,

i) Aufgaben gemäß den Buchstaben a) – h), soweit sie bisher von den Trägern für Dritte wahrgenommen werden.

Lt. § 4 Abs. 10 bringen die Träger Verträge bzw. Vereinbarungen gemäß Anlage 10 ein. Des Weiteren werden die Aufgaben des Datenschutzbeauftragten und weitere Aufgaben für die Amtsschulen nach § 4 Abs. 1 an das gemeinsame Kommunalunternehmen übertragen.

„Ist Gegenstand des Vertrages zwischen Verantwortlichem und Auftragsverarbeiter die IT-Wartung oder Fernwartung (z. B. Fehleranalysen, Support-Arbeiten an Systemen des Auftraggebers) und besteht in diesem Rahmen für den Auftragsverarbeiter die Notwendigkeit oder Möglichkeit des Zugriffs auf personenbezogene Daten, so handelt es sich im Hinblick auf die weite Definition einer Verarbeitung in Art. 4 Nr. 2 DS-GVO (z. B. Auslesen, Abfragen, Verwenden) ebenfalls um eine Form oder Teiltätigkeit einer Auftragsverarbeitung und die Anforderungen des Art. 28 DS-GVO – wie etwa der Abschluss eines Vertrages zur Auftragsverarbeitung – sind umzusetzen."[4]

P 2 *Der Vertrag zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO, die technischen und organisatorischen Maßnahmen des Auftragnehmers gemäß Art. 32 DS-GVO sowie die Richtlinie zur Durchführung von Fernwartungen mittels VPN Zugang gemäß Art. 28 DS-GVO wurden nicht vorgelegt.*

2.3 Dienstleistungsvertrag

Zur technischen Unterstützung wird ein externes IT-Dienstleistungsunternehmen herangezogen. Gemäß § 21 GemHVO-Doppik M-V und § 9 Abs. 1 S. 3 VOL/A waren die „Ergänzenden

[4] Datenschutzkonferenz, Kurzpapier Nr. 13 vom 16.01.2018, https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Kurzpapiere/Kurzpapier_Nr_13.pdf, (Abrufdatum: 20.08.2020)

Vertragsbedingungen" verbindlich anzuwenden. Das gestiegene Sicherheitsinteresse der öffentlichen Auftraggeber wird durch die standardisierten EVB-IT Verträge, u. a. zu den Nutzungsrechten, Verzug, Gewährleistung und Haftungsansprüchen sichergestellt. Weitere Informationen sind auf der Internetseite „Der Beauftragte der Bundesregierung für Informationstechnik"[5] aufgeführt.

Zur Prüfung wurde der EVB-IT Instandhaltungsvertrag vom 01.12.2017 vorgelegt. Es gab keine Beanstandung.

Zur Durchführung von Updates, Wartungsarbeiten, Mängelbeseitigung, Support-Maßnahmen und zur Überprüfung der IT-Infrastruktur können sich die Mitarbeiter des Dienstleisters auf das IT-System des Amtes Stralendorf schalten. Hinreichende Erläuterungen zur Auftragsverarbeitung erfolgten bereits unter Punkt 2.2.

Zur Prüfung wurde der Vertrag zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO, die technischen und organisatorischen Maßnahmen des Auftragnehmers gemäß Art. 32 DS-GVO und die Richtlinie zur Durchführung von Fernwartungen mittels VPN Zugang gemäß Art. 28 DS-GVO angefordert.

Zur Prüfung wurden vorgelegt:

- der Vertrag zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO vom 11.06.2018 sowie
- die technischen und organisatorischen Maßnahmen des Auftragnehmers gemäß Art. 32 DS-GVO.

P *Die Richtlinie zur Durchführung von Fernwartungen mittels VPN Zugang gemäß Art. 28 DS-GVO wurde nicht vorgelegt.*

2.4 Datenschutz

Auf Grund des zunehmenden Bedrohungspotentials wird ein konsequenter Datenschutz weiter an Bedeutung zunehmen. Die Einhaltung der Vorschriften zum Datenschutz ist eine originäre Aufgabe der Verwaltungsführung. Ihr obliegt die Verantwortung zur Datenschutzklassifikation von Anwendungen bzw. personenbezogenen Daten und die Bestimmung sowie die Überwachung des Sicherheits- und Schutzniveaus.[6] Ein DSB ist lt. Art. 37 DS-GVO zu benennen.

Mit Schließung des öffentlich-rechtlichen Vertrages zur Beteiligung des Amtes Stralendorf an die KSM AöR vom 18.12.2019 wurden die Aufgaben des Datenschutzbeauftragten zum 01.01.2020 an das gemeinsame Kommunalunternehmen übertragen. Die bisherige Vertragspartnerschaft mit dem ZV eGov MV wurde zum 31.12.2019 gekündigt. Zur realistischen Einschätzung eines effizienten und effektiven Datenschutzes in der Amtsverwaltung wurden die Ergebnisse zur Einhaltung der datenschutzrechtlichen Vorgaben der vergangenen Jahre in die Prüfung einbezogen.

Zur Prüfung wurde der EVB-IT-Dienstvertrag 00000099/001/009 mit dem ZV eGO-M-V vorgelegt. Der Vertrag wurde mit Datum vom 17.07.2013 geschlossen. Lt. Vertragsgegenstand wurden nachfolgende Sachverhalte vereinbart:

- der Aufragnehmer stellt dem Auftraggeber einen GDSB,
- der Auftraggeber bestellt schriftlich einen stellvertretenden DSB.

[5] Der Beauftragte der Bundesregierung für Informationstechnik; https://www.cio.bund.de/Web/DE/IT-Beschaffung/it_beschaffung_node.html (Abrufdatum: 14.06.2020)

[6] IT-Governance in Staat und Kommunen, Andreas Engel, Seite 125, Datenschutz

H Bis zum 24.05.2018 war lt. § 20 DSG M-V für die Bestellung eines DSB die Schriftform vorgeschrieben. Der Art. 37 Abs. 1 DS-GVO spricht lediglich von einer Benennung des DSB. Aus Beweisgründen im Hinblick auf die Nachweispflichten gemäß Art. 24 Abs. 1 DS-GVO und Art. 5 Abs. 2 DS-GVO und zur Rechtssicherheit ist es jedoch empfehlenswert, die Benennung eines DSB in geeigneter Form zu dokumentieren. Die bereits vor Geltung der DS-GVO unterzeichneten Bestellungsurkunden gelten vor diesem Hintergrund fort. Die Urkunde und etwaige darin enthaltenen Zusatzvereinbarungen und Aufgabenzuweisungen sollten auf ihre Vereinbarkeit mit den neuen Regelungen der DS-GVO überprüft und ggf. angepasst werden.[7]

Zur Überprüfung wurden die Bestellung der GDSB und der stellvertretenden DSB angefordert. Es wurde die Bestellung des DSB des Amtes Stralendorf vom 19.11.2002 vorgelegt.

P *Die Bestellung des GDSB sowie des stellvertretenden DSB gemäß EVB-IT-Dienstvertrag vom 17.07.2013 wurden nicht vorgelegt.*

P 3 *Die Bestellung des GDSB sowie des stellvertretenden DSB wurden nicht vorgelegt. Es ist davon auszugehen, dass nach den vorliegenden Dokumenten derzeit der Datenschutzbeauftragte des Amtes Stralendorf, Bestellurkunde vom 19.11.2002, als Datenschutzbeauftragter des Amtes Stralendorf eingesetzt ist, was der vertraglichen Situation widerspricht. Dieser Zustand ist umgehend zu ändern.*

Als zentrales Prinzip des Datenschutzes wurde in der DS-GVO auch die Gewährleistung von Datensicherheit verankert. Dokumentations- und Rechenschaftspflichten wurden in Art. 5 Abs. 2 und Art. 32 Abs. 1 d) DS-GVO festgelegt. Zur Überprüfung eines effektiven Datenschutzes innerhalb der Amtsverwaltung wurde der Maßnahmeplan zum Datenschutz und Datensicherheit angefordert. Es wurde der Maßnahmeplan mit Stand vom 15.02.2012 übergeben.

Es wurden folgende Maßnahmen überprüft:

- Regelungen für Wartungs- und Reparaturarbeiten
  Erstellung einer Dokumentation zu Reparatur- und Wartungsarbeiten sowie für die Fernwartung. Die Maßnahme wurde als „erledigt" gekennzeichnet.

P *Die Dokumentation zu Reparatur- und Wartungsarbeiten sowie für die Fernwartung fehlt.*

- Maßnahme Infrastruktur, Brandschutz, USV
  Einbau einer Brandschutztür. Die Maßnahme wurde mit Datum „2012" gekennzeichnet.

P *Die Maßnahme „Einbau einer Brandschutztür" für den Serverraum wurde nicht durchgeführt.*

- Maßnahme Vergabe von Zugangs- und Zugriffsrechten
  Erstellung eines Formulars zur Erteilung und den Entzug von Zugangs- und Zugriffsrechten. Die Maßnahme wurde als „erledigt" gekennzeichnet. Die DA Nr. 3 zur Regelung des Einsatzes der Informationstechnik und zum Datenschutz im Amt Stralendorf vom 30.04.2018 verweist auf die Anlage 3 zur Erteilung und den Entzug von Zugangs- und Zugriffsrechten. Es gab keine Beanstandung.

P 4 *Ein effizienter und effektiver Datenschutz liegt derzeit in der Amtsverwaltung Stralendorf nicht vor.*

[7] Kurzpapier Nr. 12: Datenschutzbeauftragter, Form der Benennung, https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Kurzpapiere/Kurzpapier_Nr_12.pdf/ Abrufdatum 20.08.2020

H Um einen effektiven Datenschutz sicherzustellen, ist ein jährlicher Maßnahmeplan zum Datenschutz und Datensicherheit für das Amt Stralendorf, der die Risiken für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit[8] von Informationen und Informationstechnik aufzeigt, zu erstellen. Eine Reduzierung von Risiken kann durch technische und organisatorische Maßnahmen auf ein akzeptierbares Maß sichergestellt werden.

2.5 Dienstvereinbarungen und -anweisungen

Zur Prüfung wurden nachfolgende DA übergeben:

- DA Nr. 3 zur Regelung des Einsatzes der Informationstechnik und zum Datenschutz im Amt Stralendorf vom 30.04.2018,
- DA Nr. 4 Nutzung von Internetdiensten vom 01.05.2013.

In der DA Nr. 3 zur Regelung des Einsatzes der Informationstechnik und zum Datenschutz sind Regelungen des DSG M-V aufgeführt. Die aufgeführten Paragraphen des DSG M-V hatten ihre Gültigkeit bis zum 24.05.2018.

Weitere Anmerkungen:

- § 4 Pkt 4.1 (3) „Darüber hinaus sind Änderungen an der Konfiguration (z. B. durch Aufspielen zusätzlicher Programme/Dateien oder Deaktivieren von Sicherheitsfunktionen [...]) unzulässig."

  Ein direkter Zugriff auf sicherheitsrelevante Systeme sollte durch den Einsatz von IT ausgeschlossen werden.
- § 4 Pkt. 4.4 (1) „Alle Dienst- und sonstigen Räume sind – auch bei nur kurzfristigem – Verlassen abzuschließen."
- § 4 Pkt. 4.6 (1) „Beim kurzfristigen Verlassen des Arbeitsplatzes ist der Bildschirm auf die Anmeldungsmaske zu stellen [...] oder ein passwortgeschützter Bildschirmschoner zu aktivieren."

P 5 *Büroräume waren nicht verschlossen, nicht beaufsichtigt und EDV-Arbeitsplätze frei zugänglich. Es wurde gegen die DA Nr. 3 zur Regelung des Einsatzes der Informationstechnik und zum Datenschutz im Amt Stralendorf vom 30.04.2018 verstoßen. Der Grundsatz der Vertraulichkeit wurde nicht beachtet.*

- § 4 Pkt. 4.4 (3) „[...] Muss das Passwort ausnahmsweise im Vertretungsfall an den Vertreter weitergegeben werden, [...]."

  Jeder Benutzer ist mit den Zugriffsrechten auszustatten, die unmittelbar für die Erledigung seiner Aufgaben notwendig sind. Es ist ein Verbot für die Weitergabe von Benutzern und deren Passwörtern festzulegen.

P 6 *Die DA Nr. 3 zur Regelung des Einsatzes der Informationstechnik und zum Datenschutz im Amt Stralendorf vom 30.04.2018 entspricht nicht den Regelungen der DS-GVO. Des Weiteren ist die Anpassung an den heutigen IT-Einsatz vorzunehmen.*

H IT-Sicherheit kann auch bei besten technischen Maßnahmen nur funktionieren, wenn die Bediensteten ein ausgeprägtes Sicherheitsbewusstsein besitzen. Die Einhaltung interner Regelungen zum IT-Einsatz ist zu verpflichten.

[8] Das Standard-Datenschutzmodell; V.20b –Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele unabhängigen Datenschutzbehörden des Bundes und der Länder, beschlossen am 17.04.2020/ https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/ Abrufdatum 20.08.2020

H In der DA Nr. 3 zur Regelung des Einsatzes der Informationstechnik und zum Datenschutz im Amt Stralendorf vom 30.04.2018 ergeben sich durch die Festlegung von Kontrollmaßnahmen unter § 5 mitbestimmungspflichtige Maßnahmen gemäß § 62 Abs. 1 und § 70 Abs. 1 Nr. 1 und 2 PersVG M-V. Ein Mitbestimmungsrecht kann nicht umgangen werden, d. h., dass der Arbeitgeber und der Personalrat eine Vereinbarung abschließen müssen.

2.6 Betriebsdokumentation

Eine notwendige Bestandsaufnahme der aufbau- und ablauforganisatorischen Organisationsstrukturen der IT-Systeme ist in der Amtsverwaltung vorzuhalten. Eine Bestandsaufnahme sollte u. a. umfassen:

- Strukturierung des Netzwerkes (physische und virtuelle Technik),
- physikalischer Netzwerkplan (aktive und passive Komponenten, LAN),
- logischer Netzwerkplan,
- Active Directory,
- Internetanbindung,
- Mailversand,
- Schema Virenschutz.

Zur Prüfung wurde die Netzwerkdokumentation des Amtes Stralendorf V2.03 vom 30.10.2019 vorgelegt. Eine Betriebsdokumentation wird vorgehalten.

2.7 Benutzerkonzept als zentraler Teil der Zugangskontrolle

Wer einen Rechner oder Rechnerdienst im IT-Netz der Verwaltung nutzen möchte, muss eine Nutzungserlaubnis für das jeweilige Rechnersystem haben, die durch die Registrierung einer Benutzerkennung und deren Zuordnung zu einer oder mehreren Nutzerkonten bzw. Netzwerkressourcen erteilt wird. Der Nutzer muss sich mit seiner Benutzerkennung am IT-System anmelden. Die Bestätigung der Identität erfolgt durch die Eingabe eines in dem jeweiligen System verschlüsselt gespeicherten Passwortes. Zur Prüfung wurde das Benutzerkonzept der Amtsverwaltung angefordert.

P 7 *Ein Benutzerkonzept für die IT-Systeme des Amtes Stralendorf lag nicht vor.*

H Im EDV-System der Amtsverwaltung sind sensible Finanz- und Kundendaten gespeichert. Daher müssen die Verantwortlichen gewährleisten, dass nur berechtigte Nutzer Zugriff auf diese Informationen erhalten. Es ist zu regeln, wie Benutzer und Benutzergruppen einzurichten sind. Ein Benutzerkonzept ist zu beschreiben.

In der Netzwerkdokumentation des Amtes Stralendorf V2.03 vom 30.10.2019 wurden die eingerichteten Computer-, Benutzer- bzw. Gruppenkonten dokumentiert.

Die Befragung über die Passwortkonventionen von Bediensteten ergab

- eine Passwortlänge von 5, 6, 8, und 9 Zeichen,
- eine Eingabe von Buchstaben (klein und groß), Sonderzeichen und Zahlen, wobei ein Zwang von Zeichen ausgeschlossen wurde,
- keinen erzwungenen Passwortwechsel durch das IT-System. Ein Bediensteter meinte, er hätte sein Passwort seit 2001 nicht geändert.

In der DA Nr. 3 zur Regelung des Einsatzes der Informationstechnik und zum Datenschutz im Amt Stralendorf vom 30.04.2018 wurden die Richtlinien zum Umgang mit den Passwörtern unter § 4 Pkt. 4.7 festgelegt.

P 8 *Die in der DA Nr. 3 zur Regelung des Einsatzes der Informationstechnik und zum Datenschutz im Amt Stralendorf vom 30.04.2018 festgelegten Passwortrichtlinien wurden nicht konsequent angewendet. Der Grundsatz der Vertraulichkeit wurde nicht beachtet.*

H Die Einhaltung der Passwortrichtlinie ist durch organisatorische und technische Maßnahmen zu forcieren.

2.8 Datensicherung

Mit der Prüfungsankündigung wurde das Datensicherungskonzept des Amtes Stralendorf angefordert. Das Datensicherungskonzept des Amtes Stralendorf wurde in der Netzwerkdokumentation des Amtes Stralendorf V2.03 vom 30.10.2019 dokumentiert. Ein Datensicherungskonzept lag vor.

2.9 Managementsystem für Informationssicherheit – ISMS

Mit Umsetzung der Leitlinie für Informationssicherheit[9] wurden die einheitlichen Sicherheitsstandards für Bund und Länder verbindlich beschrieben. Durch die gemeinsame Nutzung von Netzinfrastrukturen und ebenenübergreifenden IT-Verfahren, sind die Sicherheitsstandards auf die Kommunalverwaltungen übertragbar und somit auch durch diese sicherzustellen. Ein ISMS ist auf Basis der Grundschutzkataloge des BSI oder der ISO 27001 in den Kommunalverwaltungen einzurichten.

Mit Schließung des öffentlich-rechtlichen Vertrages zur Beteiligung des Amtes Stralendorf an die KSM AöR vom 18.12.2019 wurde die Systembetreuung für IT-Verfahren und -Systeme inklusive IT-Sicherheit und IT-Sicherheitsbeauftragten zum 01.01.2020 an das gemeinsame Kommunalunternehmen übertragen. Die bisherige Vertragspartnerschaft mit dem ZV eGov MV wurde zum 31.12.2019 gekündigt.

Zur Prüfung wurde die Bestandsaufnahme zur Datenschutzorganisation und IT Sicherheit von März 2010 übergeben. Des Weiteren wurde der EVB-IT Dienstvertrag 2017/99/0088 über die Nutzung eines IT-Sicherheitsbeauftragten vom 14.11.2016 vorgelegt.

P 9 *Ein Management für Informationssicherheit – ISMS fehlt.*

H Die Planung, Umsetzung, Überprüfung und Verbesserung der Informationssicherheit darf nicht als ein Projekt angesehen werden, das nach einem festen Terminplan durchgeführt wird und die Zielstellung hat, für mehr Informationssicherheit zu sorgen. Vielmehr handelt es sich um einen Prozess zur Feststellung des aktuellen Sicherheitsniveaus und daraus resultierenden Festlegungen zur Verbesserung. Die Einführung und Aufrechterhaltung dieses Sicherheitsprozesses ist Aufgabe der Behördenleitung. Sie muss den Sicherheitsprozess initiieren, steuern und auch überprüfen, ob die Sicherheitsziele in allen Bereichen umgesetzt werden. Nur wenn sie voll hinter den Sicherheitszielen und den damit verbundenen Aktivitäten steht, kann diese Aufgabe erfolgreich wahrgenommen werden. Dafür ist eine systematische Herangehensweise an einen kontinuierlichen Überwachungs- und Optimierungsprozess nötig, mit dem sowohl die Technik als auch die Beschäftigten und weitere Einflussfaktoren berücksichtigt werden.[10] Als Grundwerte der Informationssicherheit gelten Integrität,

[9] Leitlinie für Informationssicherheit in der öffentlichen Verwaltung; Informationssicherheit des IT Planungsrates, https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2019/Sitzung_28.html?pos=4 (Abrufdatum: 20.08.2020) https://www.it-planungsrat.de/SharedDocs/Sitzungen/DE/2020/Sitzung_31.html?pos=4 (Abrufdatum: 20.08.2020)

[10] Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen

Vertraulichkeit und Verfügbarkeit. Die Absicherung dieser Grundwerte ist durch entsprechende Maßnahmen abzusichern.

2.10 Sicherheit der Infrastruktur

Die Prüfung bezog sich ausschließlich auf den Verwaltungssitz.

Die ebenerdige Bauweise des Verwaltungsgebäudes bietet weite Blicke in Büroräume. Von außen konnte ein Technikraum lokalisiert und auf einen 27 Zoll Widescreen TFT Monitor geschaut werden. Auf das Risiko von Informationsverlusten bzw. Sabotage wurde aufmerksam gemacht. Während der Prüfung wurden die Risiken beseitigt.

P *Der Grundsatz der Vertraulichkeit, Schutz für die Verarbeitungstätigkeit ausgestatteter Umgebungen, wurde nicht beachtet.*

Des Weiteren wurde der derzeitige Serverraum und der zukünftige Technikraum geprüft.

Serverraum/ IT-Technikraum

Die Prüfungen basieren beispielhaft auf den Fragestellungen der BSI-Vorgaben INF.2, technische und organisatorische Vorgaben für Serverräume.

1. War der Serverraum/ IT-Technikraum bei Begutachtung verschlossen?

   Ja, der Serverraum/ IT-Technikraum war verschlossen.

2. War im Serverraum eine Klimaanlage installiert?

   Eine Klimaanlage war installiert.

3. Werden die Zutritte zum Serverraum/ IT-Technikraum elektronisch kontrolliert?

   Es sind keine elektronischen Zugangssysteme installiert.

3. Weisen die Türen, Fenster und Wände einen ausreichenden Einbruch-, Rauch- und Feuerschutz auf?

   Nein.

3. Sind bei der Auswahl der Räumlichkeiten Gefährdungen durch Umgebungseinflüsse weitgehend vermieden worden?

   Nein.

4. Ist bei der Planung berücksichtigt worden, dass die Trassen der Versorgungsleitungen nicht in unmittelbarer Nähe oder gar durch sensible Bereiche verlaufen?

   Nein.

P 10 *Der Serverraum/ IT-Technikraum wurde nicht als geschlossener Sicherheitsbereich installiert.*

H Ein Serverraum bzw. IT-Technikraum ist ein sicherheitsrelevanter Bereich, daher sollten dort nur die Administratoren und Berechtigte Zutritt haben. In einem Serverraum sollten sich auf keinen Fall Geräte oder Ausrüstungen befinden, die den Zutritt für einen großen Benutzerkreis erforderlich machen. Brennbare Materialen sollten sich ebenfalls nicht darin befinden. Der Schutz der Infrastruktur ist herzustellen.

2.11 Rechnungswesen

Die Finanzanwendung ist ein Hauptverfahren der Verwaltung. Zahlungen aus anderen FD der Amtsverwaltung oder deren Fachanwendungen können nur durch Beteiligung des Fachdienstes Finanzen, Liegenschaften bzw. Amtskasse und der Buchung der Zahlungsströme in der Finanzanwendung bewirkt werden. Die Finanzanwendung „H&H proDoppik" V4.0 wurde für

die Fertigstellung der Planung und Eröffnung des ersten doppischen HHJ 2012 installiert. Die Implementierung der Stammdaten wurde wirksam vorgenommen.

Werden die Kassengeschäfte oder das Rechnungswesen ganz oder zum Teil automatisiert, sind die Programme gemäß § 59 Abs. 2 KV M-V vor ihrer Anwendung vom Anwender zu prüfen und vom LVB freizugeben.

Zum Prüfungszeitpunkt war die Finanzanwendung „H&H proDoppik" V4.10 A12 installiert. Die Übersicht über die installierten Versionen lag vor. Es gab keine Beanstandung.

Aus den GoBD ist zu entnehmen:

„Die Nachprüfbarkeit der Bücher und sonst erforderlichen Aufzeichnungen erfordert eine aussagekräftige und vollständige Verfahrensdokumentation, die sowohl die aktuellen als auch die historischen Verfahrensinhalte für die Dauer der Aufbewahrungsfrist nachweist und den in der Praxis eingesetzten Versionen des DV-Systems entspricht."

Die Verfahrensdokumentation über das Finanzwesen besteht aus der Anwenderdokumentation und der technischen Systemdokumentation sowie der Betriebsdokumentation.[11]

Eine Betriebsdokumentation über das Rechnungswesen wurde nicht vorgelegt.

P 11 *Die Verfahrensdokumentation für das Rechnungswesen ist unvollständig.*

H Eine Verfahrensbeschreibung ist vollständig und aktuell, wenn alle Verarbeitungsprozesse mit allen rechtlichen Forderungen und allen Daten, Systemen und Prozessen so erfasst sind, dass der Produktivbetrieb einer Organisation hinreichend genau und den tatsächlichen Gegebenheiten entsprechend beschrieben ist und alle Maßnahmen entsprechend dem festgelegten Schutzbedarf mit ihrem Erfüllungsgrad dargestellt sind. Der Grundsatz der Vollständigkeit und Aktualität ist anzuwenden.[12]

H Es müssen organisatorische Maßnahmen zur Sicherung aller Aufzeichnungen und Unterlagen getroffen werden. Auch ein unverschuldeter Verlust von aufbewahrungspflichtigen Unterlagen nimmt der Buchführung ihre Ordnungsmäßigkeit.

Das Finanzwesen war zum Prüfungszeitpunkt mit nachfolgenden Softwarekomponenten lauffähig installiert:

- Serverbetriebssystem Microsoft Windows 2012 R2 - Fachanwendung,
- Serverbetriebssystem Microsoft Windows 2012 R2 - Datenbank,
- Datenbank Progress V11.7.3.006,
- Client – Windows 7, MS Office 2010, Windows 10, MS Office 2016,
- Bankensoftware SFIRM V3.2 Patch 30.

P 12 *Für das eingesetzte Betriebssystem Microsoft Windows 7 endete der erweiterte Support durch den Hersteller am 14.01.2020. Die Sicherheitslücken sind zeitnah durch den Umstieg auf ein aktuelles Betriebssystem zu schließen.*

H Der erweiterte Support für Microsoft Office 2010 endet am 13.10.2020.

Nachfolgende Schnittstellen zu und von anderen Anwendungen wurden u. a. in der Amtsverwaltung Stralendorf installiert:

- Lohn- und Gehaltsabrechnung (BVL-Lohn),
- Wohngeld,
- Archikart (Grundstücks- und Liegenschaftsverwaltung),

[11] IDW RS FAIT 1 Pkt. 3.2.5 (54)

[12] Rundschreiben Nr. 1/2019 des Landesrechnungshofes M-V, Ordnungsmäßigkeit des Einsatzes von Informationstechnik vom 16.04.2019, Grundsatz der Vollständigkeit und Aktualität

- Session (Sitzungsmanagement),
- KITA (Kindertagesstätte),
- EC (EC-Cash),
- SFIRM.

Die Bezeichnungen wurden aus der Fachanwendung „H&H proDoppik" übernommen.

Laut Netzwerkdokumentation des Amtes Stralendorf V2.03 vom 30.10.2019 bilden u. a. nachfolgende Fachanwendungen finanzrelevante Geschäftsabläufe in automatisierten Fachanwendungen elektronisch ab:

- Gewerbe-/ Gaststättenverfahren - GESO,
- Wohngeld – IKOL-WG,
- MESO - Melde-/ Personalausweis-/Passverfahren.

Werden für die Ermittlung von Ansprüchen und Zahlungsverpflichtungen automatisierte Verfahren eingesetzt, ist der § 12 Abs. 1 GemKVO-Doppik M-V anzuwenden.

P 13 *Für Fachanwendungen, die finanzrelevante Geschäftsabläufe elektronisch abbilden, lagen seit Einführung der Doppik keine Freigaben gemäß § 12 Abs. 1 GemKVO-Doppik M-V vor.*

Für die Finanzanwendung „H&H proDoppik" wurde eine Testumgebung eingerichtet. Die Abwicklung der elektronischen Kontoführung sowie des elektronischen Zahlungsverkehrs mit Banken erfolgt durch den Einsatz der multibankenfähigen Electronic-Banking-Software SFIRM. Die Finanzverantwortung ist zentral organisiert.

Laut § 26 Abs. 10 GemHVO-Doppik M-V i. V. m. § 12 Abs. 1 Nr. 3 GemKVO-Doppik M-V und § 28 Abs. 2 Nr. 2d) GemHVO-Doppik M-V ist nachvollziehbar zu dokumentieren, wer wann welche Daten eingegeben oder verändert hat. In der Verfahrensdokumentation (P 11) sind die ablauforganisatorischen Festlegungen zu beschreiben. Die Aktivierung des Protokolls wurde überprüft. Es gab keine Beanstandung.

2.11.1 Verträge

Gemäß § 21 GemHVO-Doppik M-V und § 9 Abs. 1 S. 3 VOL/A waren die „Ergänzenden Vertragsbedingungen" verbindlich anzuwenden.

Zur Prüfung wurden für die Finanzanwendung

- der BVB Vertrag vom 05.12.2001,
- der EVB-IT Pflegevertrag für Standardsoftware, Vertragsnummer 10381-2010 vom 20.07.2010,
- die Ergänzenden Vertragsbedingungen für die Pflege von Standardsoftware sowie
- der Lizenzschein „H&H proDoppik" vom 05.02.2018 vorgelegt.

Die Bezeichnungen wurden aus den Verträgen übernommen.

Das einheitliche EVB-IT Vertragsmuster ist Grundlage des EVB-IT Pflegevertrages vom 20.07.2010. Es gab keine Beanstandung.

Zur Durchführung von Wartungsarbeiten oder Mängelbeseitigung können sich Mitarbeiter des Softwareunternehmens auf das IT-System des Amtes Stralendorf schalten. Hinreichende Erläuterungen zur Auftragsverarbeitung erfolgten bereits unter Punkt 2.2.

Zur Prüfung wurde der Vertrag zur Auftragsverarbeitung zwischen dem Amt Stralendorf und H&H mbH vom 16.05.2018 gemäß Art. 28 DS-GVO sowie die Richtlinie zur Durchführung von Fernwartungen mittels VPN Zugang und die technischen und organisatorischen Maßnahmen des Auftragnehmers gemäß Art. 32 DS-GVO vorgelegt. Es gab keine Beanstandung.

2.11.2 Fachliche Vorabprüfung

Mit Einführung des NKHR-MV sind die in den Städten und Ämtern eingesetzten EDV-Systeme durch den Anwender daraufhin zu überprüfen, ob sie die Anforderungen, die das NKHR-MV an die Haushaltsplanung, die Haushaltsüberwachung sowie das Rechnungswesen stellt, erfüllen können. Laut § 59 Abs. 2 KV M-V, § 28 Abs. 2 Nr. 2a) GemHVO-Doppik M-V sowie § 26 Abs. 10 GemHVO-Doppik M-V i. V. m. § 12 Abs. 1 Nr. 1 GemKVO-Doppik M-V sind nur gültige Programme, die vom Anwender fachlich geprüft wurden, zu verwenden. Der Anwender handelt gesetzeskonform, indem er entweder die Finanzanwendung fachlich selbst prüft oder sich dafür eines beauftragten Dritten bedient. Beide Prüfungsverfahren müssen auf der Basis eines Anforderungskataloges für Fachprogramme „Doppisches Finanzwesen" in der öffentlichen Verwaltung ein Test- und Freigabeverfahren durchführen. Im Ergebnis ist der Testgegenstand, Art und Umfang der Testfälle sowie die Dokumentation und die Archivierung der Testergebnisse zu dokumentieren. Neben der Dokumentation über die Programmprüfung hat der Kämmerer bzw. der Leiter Finanzen die Eignung des Programmes zu bestätigen.[13]

H Lt. VV zu § 34 GemKVO-Doppik M-V „ist der Leitfaden zur Erstellung von DA zur Organisation des Rechnungswesens (Anlage 4) zu beachten und entsprechend der örtlichen Organisation anzuwenden.".

Zum anderen könnten die Empfehlungen der Zertifizierungsstelle TÜV Informationstechnik GmbH auf der Grundlage der OKKSA–Anforderungskataloge genutzt werden. Durch die Softwarezertifizierung wird Programmbenutzern und Prüfstellen eine Orientierung auf die einheitliche Feststellung der Eignung von Programmen ermöglicht. Zumindest wird ein Qualitätsniveau zertifiziert, welches vorhanden sein müsste, um ein rechts- und normenkonformes Arbeiten mit der Software sicherzustellen. Zu beachten wäre, dass die Normen auf Anregung und durch die Initiative interessierter Kreise entstehen. Als solches können diese Zertifikate hinter den laufenden Lizenzversionen zurückbleiben. Als Entscheidungsmerkmal für den Einsatz einer neuen Finanzanwendung bzw. einem Releasewechsel können diese Zertifikate durchaus dienlich sein. Sie ersetzen aber grundsätzlich nicht die Anforderungen aus dem Gesetz.[14] Die Finanzanwendung „H&H pro-Doppik" V4.0 wurde für die Fertigstellung der Planung und Eröffnung des ersten doppischen HHJ 2012 installiert. Eine Sichtung der Zertifizierung ergab, dass die V4.0 für M-V durch die Zertifizierungsstelle der TÜV Informationstechnik GmbH vom 29.11.2010 bis zum 30.11.2013 zertifiziert wurde. Gültige Zertifikate konnten demzufolge herangezogen werden.

Sachrelevante Dokumentationen über eine Vorabprüfung für die im Rechnungswesen eingesetzten DV-Programme konnten nicht vorgelegt werden.

P 14 *Die ordnungsgemäße fachliche Vorabprüfung wurde nicht durchgeführt.*

H Im Ergebnis hätte weder die Freigabe noch die Aufnahme der Arbeit im Produktivsystem für die im Rechnungswesen eingesetzten DV-Programme erfolgen dürfen. Dafür sprechen auch die Prüfungsbeanstandungen aus dem Bericht über die Prüfung der HH-Jahre 2015 bis 2018 des Amtes Stralendorf, Pkt. 3.3.5.2 Plausibilitätsprüfung. Gemäß § 12 Abs. 1 Nr. 2 GemKVO-Doppik M-V sind organisatorische Festlegungen zu treffen, die sicherstellen, dass die Daten vollständig und richtig erfasst, eingegeben, verarbeitet und ausgegeben werden. Der Grundsatz der Integrität, Sicherstellung der Korrektheit von Daten und Systemen, wurde nicht beachtet.

[13] Verwaltungsvorschrift des Innenministeriums vom 8. Dezember 2008 – II 320-174.3.2.1 Anlage 4, Punkt 7.1.3

[14] Handbuch für das Kassen- und Rechnungswesen, Punkt 25.8.2.1

2.11.3 Verzeichnis über die Verarbeitungstätigkeiten

Die datenverarbeitende Stelle war lt. § 18 Abs. 1 DSG M-V bis zum 24.05.2018 verpflichtet, eine Verfahrensbeschreibung zu führen. Weitere Regelungen aus § 18 Absatz 1 Nr. 7 DSG M-V sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach den §§ 21 und 22 DSG M-V waren zu beachten. Aus § 21 DSG M-V ergeben sich die allgemeinen Maßnahmen zur Datensicherheit, Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität der Daten, Revisionsfähigkeit und Transparenz und aus § 22 DSG M-V die besonderen Maßnahmen zur Datensicherheit beim Einsatz automatisierter Verfahren. Insbesondere war gemäß § 22 Abs. 5 DSG M-V für automatisierte Verfahren ein Sicherheitskonzept vorzuhalten.

Seit dem 25.5.2018 muss in vielerlei Hinsicht detailliert belegt werden können, dass personenbezogene Daten in Einklang mit der DS-GVO verarbeitet werden. Die Verfahrensbeschreibung wird zum Verzeichnis über die Verarbeitungstätigkeiten. Die technischen und organisatorischen Maßnahmen sind lt. Art. 32 DS-GVO vorzunehmen. Eine Datenschutz-Folgenabschätzung ist nach Art. 35 DS-GVO durchzuführen. Zur Prüfung wurden die Leitlinien zur Datenschutz-Folgenabschätzung WP248 Rev. 01[15] herangezogen.

Zum Prüfungszeitpunkt wurden keine Unterlagen zu v.g. Sachverhalten vorgelegt.

P *Die Verfahrensbeschreibung gemäß § 18 DSG M-V sowie die technischen und organisatorischen Maßnahmen nach §§ 21 und 22 DSG M-V lagen zur Einführung der Doppik nicht vor.*

P *Für das Rechnungswesen lag kein Sicherheitskonzept vor.*

P 15 *Das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO sowie die Anlage technische und organisatorische Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO zum Verzeichnis von Verarbeitungstätigkeiten fehlen.*

H Die Anforderungen der GoBD an eine ordnungsgemäße IT-gestützte Rechnungslegung für alle Elemente des IT-Systems sind sicherzustellen. Diese sind zugleich eine wesentliche Bedingung für die angemessene Umsetzung eines Sicherheitskonzepts.[16]

P 16 *Die Datenschutz-Folgenabschätzung für die Finanzanwendung „H&H proDoppik" gemäß Art. 35 DS-GVO fehlt.*

H Eine Verletzung der Sicherheit der Datenverarbeitung ist immer eine Verletzung des Schutzes personenbezogener Daten i. S. v. Art. 4 Nr. 12 DS-GVO.[17]

2.11.4 Benutzerrechte

Der FD Finanzen, Liegenschaften stellt allen FD wesentliche Finanzinformationen zur Verfügung. Gemäß § 28 Abs. 2 Nr. 2c) GemHVO-Doppik M-V sowie § 26 Abs. 10 GemHVO-Doppik M-V i. V. m. § 12 Abs. 1 Nr. 4 und 5 GemKVO-Doppik M-V darf in automatisierte Verfahren nicht unbefugt eingegriffen werden bzw. dürfen gespeicherte Informationen nicht unbefugt verändert oder gelöscht werden. Die Finanzanwendung verfügt über eine zentrale Benutzer- und Rechteverwaltung. Für jeden zur Anwendung zugelassenen Benutzer muss ein eindeutiger

[15] Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt" vom 04. April 2017

[16] IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)

[17] Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO, Stand Februar 2018, Datenschutzkonferenz https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/HilfsmittelzurUmsetzung/VVT/HinweiseZumVerzeichnisvonVerarbeitungstaetigkeiten.pdf (Abrufdatum: 20.11.2020)

Login-Name festgelegt werden. Über zugewiesenen Gruppenberechtigungen können erweiterte Verfügungsberechtigungen für Benutzer erteilt oder versagt werden.

Zur Prüfung wurde das Benutzerkonzept für die Finanzanwendung der Amtsverwaltung angefordert.

P 17 *Ein Benutzerkonzept für das Rechnungswesen war zum Zeitpunkt der Prüfung nicht in Kraft. Dessen ungeachtet wurden Benutzerrechte eingerichtet und produktiv umgesetzt.*

H Gemäß § 28 Abs. 2 Nr. 2c) GemHVO-Doppik M-V ist im Haushaltsrecht das Prinzip der minimalen Berechtigung anzuwenden. Dazu muss insbesondere gewährleistet sein, dass Bedienstete Berechtigungen nicht behalten, wenn sie diese für die Erledigung einer übertragenen Aufgabe nicht mehr benötigen. Die nachträgliche Erweiterung von Berechtigungen muss ebenfalls mit dem Prinzip der minimalen Berechtigung vereinbar sein.

Die Prüfung wurde in nachfolgenden Abschnitten durchgeführt:

1. Administratoren für die Fachanwendung und deren Funktionstrennung.
2. Prüfung von Benutzerrechten an Arbeitsplätzen der Bediensteten.
3. Leserechte auf Personendaten.

Zur Prüfung wurde nachfolgend herangezogen:

- Finanzdienstanweisung zur Organisation des Rechnungswesens vom 01.01.2018 in der Fassung vom 12.04.2018,
- Verwaltungsstruktur vom 14.10.2019,
- das Anwenderhandbuch Personen – H&H,
- Liste der Benutzer und Benutzerberechtigungen, welche während der Prüfung aus der Finanzanwendung kopiert wurden.

Auf der Grundlage der eingerichteten Benutzer und Benutzerberechtigungen in der Finanzanwendung, wurden Kontrollen an EDV-Arbeitsplätzen in der Koordinierungsstelle, im FD II Finanzen, Liegenschaften und im FD III Bauen, Gebäudemanagement durchgeführt.

Die Prüfung führte zu folgendem Ergebnis:

- Lt. § 28 Abs. 2 Nr. 2h) GemHVO-Doppik M-V sowie § 12 Abs. 1 Nr. 11 GemKVO-Doppik M-V ist die Abgrenzung der Verwaltung von Informationssystemen und automatisierten Verfahren von der fachlichen Sachbearbeitung und der Erledigung der Aufgaben der Finanzbuchhaltung zu trennen.

P 18 *Eine Funktionstrennung ist derzeit nicht realisiert.*

- Die eingerichteten Benutzer weisen signifikant auf die berechtigten Bediensteten. Es gab keine Beanstandung.
- Zu den personenbezogenen Daten zählen beispielsweise Name, Alter, Geburtsdatum, Anschrift, Telefonnummer, E-Mail, Bankdaten und auch der Familienstand. Diese Daten werden durch die Datenschutzgesetze und deren Richtlinien geschützt. Berechtigungen sind hier besonders gründlich zu prüfen. Es gab keine Beanstandung.

H Berechtigungsprozesse, die als Basis für die Zuordnung von Berechtigungen und deren Revision dienen, sind zu beschreiben, in einem Benutzerkonzept aufzunehmen und als verbindlich festzulegen. Das Prinzip der minimalen Berechtigungsvergabe ist anzuwenden. Erteilte, entzogene bzw. modifizierte Berechtigungen sind fortlaufend zu dokumentieren. Es wird empfohlen, einmal im Jahr eine Revision über die erteilten

Berechtigungen durchzuführen. Berechtigungskonzepte zählen zu den Organisationsunterlagen der EDV-Buchführung. Aufbewahrungsfristen gemäß § 29 GemHVO-Doppik M-V sind einzuhalten.

2.11.5 Ablauforganisation Rechnungseingang und Zahlungsabwicklung innerhalb der Finanzanwendung

Entsprechend den Anweisungen aus der Finanzdienstanweisung zur Organisation des Rechnungswesens vom 01.01.2018 in der Fassung vom 12.04.2018 wurde die Ablauforganisation des Rechnungseingangs bis zur Zahlungsabwicklung geprüft.

P 19 *Aus der Finanzdienstanweisung zur Organisation des Rechnungswesens vom 01.01.2018 in der Fassung vom 12.04.2018 konnten keine Festlegungen über den Umgang mit elektronisch eingehenden originären Rechnungsbelegen im PDF-Format und der Rechnungsverarbeitung entnommen werden.*

H Die Ordnungsmäßigkeit des Einsatzes von IT setzt Dokumentationen voraus. Darin sind die aus den rechtlichen Grundlagen abgeleiteten organisatorischen und technischen Maßnahmen zu dokumentieren und notwendige behördeninterne Regelungen zu erlassen. Diese sollen einen rechtmäßigen Vollzug beim Einsatz von IT sicherstellen. Auf die P 11 zur Verfahrensdokumentation über das Rechnungswesen wird verwiesen.

2.11.6 Neuanlage und Pflege von Personenkonten

Die Neuanlage und Pflege von Personenkonten ist in der Finanzdienstanweisung zur Organisation des Rechnungswesens vom 01.01.2018 in der Fassung vom 12.04.2018, Pkt. 2.4.10 „Die Verwaltung der Personenkonten [...] ist die Aufgabe der zentralen Geschäftsbuchführung. Zur Verwaltung der Personenkonten gehört auch die Neuanlage und Pflege von Personendaten in der Finanzsoftware." geregelt. Bei der Überprüfung der Benutzerrechte wurde festgestellt, dass Bedienstete aus dem Bereich Steuern und Abgaben über Benutzerrechte zur Neuanlage und Pflege von Bürgerkonten in der Finanzanwendung verfügten.

P 20 *Es wurde gegen die Finanzdienstanweisung zur Organisation des Rechnungswesens vom 01.01.2018 in der Fassung vom 12.04.2018 verstoßen. Die DA zur Organisation des Rechnungswesens ist entsprechend zu ändern.*

2.11.7 Elektronischer Zahlungsverkehr

Seit dem DFÜ-Abkommen über die Datenfernübertragung zwischen Kunden und Kreditinstituten ist es in Deutschland möglich, den Zahlungsverkehr für die Verwaltungen elektronisch abzuwickeln. Weitere Gesetzesentwicklungen und die Erweiterungen von einheitlichen Standards ermöglichen heute die Abwicklung des elektronischen Zahlungsverkehrs sowie der elektronischen Kontoführung über internetbasierte Plattformen. Die elektronische Zahlungsabwicklung und Kontoführung im Amt Stralendorf basiert auf dem Sicherungs- und Übertragungsstandard EBICS. EBICS bietet u. a. einen wesentlichen Aspekt zur Erreichung eines hohen Niveaus an Infrastruktursicherheit bezüglich Signatur und Verschlüsselung sowie flexible Kommunikation über das Internet.

Die Softwareanwendung Electronic-Banking-Software SFIRM V3.2 Patch 30 Featurepack 3 wird zur Realisierung des elektronischen Zahlungsverkehrs genutzt. Installierte digitale Unterschriften sichern den elektronischen Geschäftsverkehr. Geprüft wurden die finanzrelevanten Geschäftsabläufe mit der Sparkasse Mecklenburg-Schwerin, Geschäftskonto 1660000951.

Zum Prüfungszeitpunkt waren 6 Benutzer im SFIRM eingerichtet. 4 Benutzer mit Vollzugriff, 1 Benutzer mit Leserechten und 1 Benutzer mit Administrationsrechten.

Prüfung

Zur Prüfung wurden nachfolgende Dokumente herangezogen:

- Finanzdienstanweisung zur Organisation des Rechnungswesens vom 01.01.2018 in der Fassung vom 12.04.2018,
- Vereinbarung über die Teilnahme an der Elektronischen Kontoführung vom 25.10.2019,
- Unterschriftskarte zum Girovertrag vom 24.10.2019,
- Konfigurationsbericht aus dem SFIRM vom 04.03.2020,
- eingerichtete Benutzerberechtigungen im Softwaremodul SFIRM vom 04.03.2020.

Geprüft wurden die Anforderungen gemäß:

- § 34 GemKVO-Doppik M-V

  Beachtung der Dienstanweisung zur ordnungsgemäßen Erledigung der Aufgaben des Kassenwesens sowie den GoB.
- § 5 Abs. 1 Nr. 2 GemKVO-Doppik M-V

  Die Datenverarbeitungseinrichtungen oder -systeme dürfen nicht unbefugt benutzt werden.
- § 28 Abs. 2 Nr. 1 b) GemHVO-Doppik M-V

  Die schriftlichen Unterschriftsbefugnisse oder die elektronischen Signaturen mit Angabe von Form und Umfang sind zu dokumentieren.
- § 28 Abs. 2 Nr. 2f) GemHVO-Doppik M-V

  Elektronische Signaturen einschließlich der Aufbewahrungsfristen müssen nachprüfbar sein.

  § 26 Abs. 10 GemHVO-Doppik M-V i. V. m. § 12 Abs. 1 Nr. 8 GemKVO-Doppik M-V

  Elektronische Signaturen müssen mindestens bis zum Ablauf der Aufbewahrungsfristen der Bücher nachprüfbar sein.
- § 29 GemHVO-Doppik M-V

  Beachtung der Aufbewahrungsfristen.
- § 18 Abs. 3 und § 12 Abs. 3 GemKVO-Doppik M-V

  Erstellung von Überweisungen im automatisierten Verfahren.
- § 5 Abs. 4 GemKVO-Doppik M-V

  Überweisungsaufträge sind von zwei Beschäftigten zu unterzeichnen. Beim Einsatz automatisierter Verfahren können die Unterschriften durch elektronische Signaturen ersetzt werden.

Die Prüfung führte zu folgendem Ergebnis:

- Laut Unterschriftskarte zum Girovertrag waren 5 Benutzer für die gemeinschaftliche elektronische Unterschrift bevollmächtigt. Die Benutzer waren eindeutig den bevollmächtigten Bediensteten zuzuordnen. Es gab keine Beanstandung.
- Die Unterschriftskarten und deren Berechtigung über die digitalen Signaturen wurden lückenlos dokumentiert und entsprechend den Aufbewahrungsfristen archiviert. Es gab keine Beanstandung.

- Das Vier-Augen-Prinzip in Form der Doppelunterschrift bzw. entsprechende elektronische Signaturen wurden beim Zahlungsverkehr eingehalten.[18] Es gab keine Beanstandung.

Die sich im Einsatz befindliche Softwareanwendung SFIRM V3.2 wurde auf die Aktualität von Patches geprüft. Seit dem 21.01.2020 liegt für SFIRM V3.2 der Patch 30 Featurepack 3 vor. Es gab keine Beanstandung.[19]

2.11.8 Freigabe

Die Anforderungen an die Freigabe des Rechnungswesens sind in mehreren Gesetzen und Rechtsverordnungen geregelt. Die haushaltsrechtliche Freigabe erfolgt gemäß § 59 Abs. 2 KV M-V, § 26 Abs. 10 GemHVO-Doppik M-V i. V. m. § 12 Abs. 1 Nr. 1 GemKVO-Doppik M-V und § 35 GemKVO-Doppik M-V sowie § 28 Abs. 2 Nr. 2b) GemHVO-Doppik M-V i. V. m. § 62 GemHVO-Doppik M-V. Unter anderem ist sicherzustellen, dass für die Freigabe der Buchführung eine aktuelle Anwender- und Verfahrensdokumentation vorliegt, die Verarbeitungsfunktionen und -regeln erfolgreich getestet und die Schnittstellenprozesse zu vor- und nachgelagerten Anwendungen funktionsfähig installiert wurden. Lt. Finanzdienstanweisung zur Organisation des Rechnungswesens vom 01.01.2018 in der Fassung vom 12.04.2018 entscheidet der LVB nach Einsicht in die Prüfungsdokumentation über den Einsatz der Programme und gibt diese zur Anwendung frei. Die datenschutzrechtliche Freigabe erfolgte bis zum 24.05.2018 gemäß § 19 Abs. 1 DSG M-V. Die Sicherstellung einer datenschutzgerechten Verarbeitung von personenbezogenen Informationen innerhalb der Finanzanwendung bzw. einer wesentlich geänderten nächsthöheren Softwareversion musste in einer Verfahrensbeschreibung lt. § 18 DSG M-V, Merkmale und Maßnahmen zur Datensicherheit, beschrieben werden. Die Freigabe erstreckte sich auf die eingesetzte Hardware, Software, den Datenbeständen und DA. Der Leiter der datenverarbeitenden Stelle oder der dafür beauftragte Vertreter hatte nach Einsicht in die Prüfungsdokumentation über den Einsatz der Programme zu entscheiden. Die Freigabe hatte schriftlich zu erfolgen. Eine mündliche Freigabe mit anschließendem Aktenvermerk war ausgeschlossen.[20]

Nachfolgende Freigabe wurde vorgelegt:

- Freigabe des Haushaltsprogramms „H&H proDoppik" der Firma H&H Datenverarbeitungs- und Beratungsgesellschaft mbH für den Einsatz beim Amt Stralendorf gemäß § 26 Abs. 10 GemHVO-Doppik M-V vom 16.01.2012.

P *Zur Einführung der Finanzanwendung „H&H proDoppik" lag keine Freigabe gemäß § 19 Abs. 1 DSG M-V vor.*

P 21 *Es lag seit Doppik-Einführung keine haushaltsrechtliche Freigabe für das Rechnungswesen gemäß § 59 Abs. 2 KV M-V vor.*

H Es lag ein Dokument zur Freigabe für die Finanzanwendung gemäß § 26 Abs. 10 GemHVO-Doppik M-V vom 16.01.2012 vor. Jedoch wurden gesetzliche Vorgaben, die für eine Freigabe einzuhalten waren, nicht umgesetzt.

H Die aufgeführten Beanstandungen unter Pkt. 2.11 (P 11-P 20) sind auszuräumen. Die ordnungsgemäße Freigabe wäre somit sichergestellt und zu dokumentieren.

[18] Hinweise zum Einsatz von Electronic-Banking-Systemen, Bayerischer Kommunales Prüfungsverband, Verfasser H. Gruschka

[19] http://www.sfirm.de/support/downloads.html

[20] Auszüge aus den Erläuterungen zur Freigabe und Vorabkontrolle i. S. d. § 19 DSGM-V, gültig bis zum 24.05.2018

3. Schlussbemerkung

Die Kommunalverwaltungen werden durch die immer komplexer werdenden IT-Infrastrukturen, die Steigerung von Cybersicherheitsvorfällen, die Abhängigkeit der Verwaltung von IT-gestützten Verfahren, die zunehmende Digitalisierung und den stetig größer werdenden Anspruch an die IT-Fachkräfte vor neue Herausforderungen gestellt. Innovationen und Digitalisierung lassen die IT-Kosten weiter steigen. Die eingeleiteten Maßnahmen in der Amtsverwaltung Stralendorf sollten konsequent fortgeführt werden.

Während der Prüfung wurden die unterschiedlichsten Themenfelder analysiert. Der Teilbericht enthält in verschiedenen Gliederungspunkten Ausführungen dazu, die als Hinweise und Prüfungsfeststellungen gekennzeichnet sind. Mit **P Ziffer** gekennzeichnete Ausführungen bedürfen einer Stellungnahme.

Abschließend bedanken wir uns für die gute Zusammenarbeit.

Parchim, den 30.11.2020
Im Auftrag

Golnik
IT-Prüferin

Vogtland
Prüfgruppenleiterin

Dittmann
Fachdienstleiter

Verteiler
Amtsvorsteher/LVB
FD 30 Recht, Kommunalaufsicht und Ordnung
Ministerium für Inneres und Europa
FD 14 Rechnungs- und Gemeindeprüfung

Protokoll vom 19.11.2020

Entwurf Teilbericht mit den Prüfungsschwerpunkten IKS, Finanzanwendung und IT im Amt Stralendorf

Anwesende:

Amt Stralendorf	:	Frau Facklam, stellv. Amtsvorsteherin
Amt Stralendorf (Verwaltung)		Herr Helterhof Leitender Verwaltungsbeamter
		Herr Borgwardt, Fachdienstleiter Finanzen Liegenschaften
		Frau Roll
		Frau Müller
Landkreis FD 30:		Frau Ziegert
FD 14:		Herr Dittmann, Fachdienstleiter
		Frau Vogtland
		Frau Felber
		Frau Golnik

Uhrzeit: 13:20 – 14:00

P 1 Die Stelle für Informationsverarbeitung war während der Prüfung personell nicht besetzt.

Protokollanmerkung: neue Stelle Digitalisierung mit VzÄ 0,5 wurde geschaffen, was aus Sicht der Prüfung auf Dauer nicht ausreichend ist; ist jedoch noch nicht besetzt (interne Umsetzung).

P 2 Der Vertrag zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DS-GVO, die technischen und organisatorischen Maßnahmen des Auftragnehmers gemäß Art. 32 DS-GVO sowie die Richtlinie zur Durchführung von Fernwartungen mittels VPN Zugang gemäß Art. 28 DS-GVO wurden nicht vorgelegt.

Protokollanmerkung: Vertragsentwurf ist bei der KSM beauftragt.

P 3 Die Bestellung des GDSB sowie des stellvertretenden DSB wurden nicht vorgelegt. Es ist davon auszugehen, dass nach den vorliegenden Dokumenten derzeit der Datenschutzbeauftragte des Amtes Stralendorf, Bestellurkunde vom 19.11.2002, als Datenschutzbeauftragter des Amtes Stralendorf eingesetzt ist, was der vertraglichen Situation widerspricht. Dieser Zustand ist umgehend zu ändern.

Protokollanmerkung: Im Prüfungszeitraum war der ZV eGov M-V für den Datenschutz zuständig. Person muss benannt werden, auch wenn sie beim IT-Dienstleister beschäftigt ist.

P 4 Ein effizienter und effektiver Datenschutz liegt derzeit in der Amtsverwaltung Stralendorf nicht vor.

Protokollanmerkung: Verbesserung wird durch Mitgliedschaft in der KSM AöR angestrebt.

P 5 Büroräume waren nicht verschlossen, nicht beaufsichtigt und EDV-Arbeitsplätze frei zugänglich. Es wurde gegen die DA Nr. 3 zur Regelung des Einsatzes der Informationstechnik und zum Datenschutz im Amt Stralendorf vom 30.04.2018 verstoßen. Der Grundsatz der Vertraulichkeit wurde nicht beachtet.

Protokollanmerkung: Es wurde bereits eine Datenschutzschulung durch den neuen DSB durchgeführt, zeitnah ist eine Begehung vorgesehen.

P 6 Die DA Nr. 3 zur Regelung des Einsatzes der Informationstechnik und zum Datenschutz im Amt Stralendorf vom 30.04.2018 entspricht nicht den Regelungen der DS-GVO. Des Weiteren ist die Anpassung an den heutigen IT-Einsatz vorzunehmen.

Protokollanmerkung: wird angepasst

P 7 Ein Benutzerkonzept für die IT-Systeme des Amtes Stralendorf lag nicht vor.

P 8 Die in der DA Nr. 3 zur Regelung des Einsatzes der Informationstechnik und zum Datenschutz im Amt Stralendorf vom 30.04.2018 festgelegten Passwortrichtlinien wurden nicht konsequent angewendet. Der Grundsatz der Vertraulichkeit wurde nicht beachtet.

Protokollanmerkung: P 7 und P 8 erledigt sich durch KSM

P 9 Ein Management für Informationssicherheit – ISMS fehlt.

Protokollanmerkung: Konzept wird inzwischen konkret auch durch EGovG M-V gefordert.

P 10 Der Serverraum/ IT-Technikraum wurde nicht als geschlossener Sicherheitsbereich installiert.

P 11 Die Verfahrensdokumentation für das Rechnungswesen ist unvollständig.

P 12 Für das eingesetzte Betriebssystem Microsoft Windows 7 endete der erweiterte Support durch den Hersteller am 14.01.2020. Die Sicherheitslücken sind zeitnah durch den Umstieg auf ein aktuelles Betriebssystem zu schließen.

Protokollanmerkung: Wird derzeit terminbasiert umgesetzt.

P 13 Für Fachanwendungen, die finanzrelevante Geschäftsabläufe elektronisch abbilden, lagen seit Einführung der Doppik keine Freigaben gemäß § 12 Abs. 1 GemKVO-Doppik M-V vor.

Protokollanmerkung: Muster für eine Freigabe nach § 59 KV M-V, § 28 GemHVO-Doppik M-V, § 12 GemKVO-Doppik M-V und der DS-GVO wird zur Verfügung gestellt.

P 14 Die ordnungsgemäße fachliche Vorabprüfung wurde nicht durchgeführt.

Protokollanmerkung: Es wird empfohlen im Verbund der KSM den EDV-Katalog des Landkreises für die Vorabprüfung des Rechnungswesens H&H zu nutzen.

P 15 Das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO sowie die Anlage technische und organisatorische Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO zum Verzeichnis von Verarbeitungstätigkeiten fehlen.

Protokollanmerkung: muss von KSM abgefordert werden.

P 16 Die Datenschutz-Folgenabschätzung für die Finanzanwendung „H&H proDoppik" gemäß Art. 35 DS-GVO fehlt.

Protokollanmerkung: kann von der KSM übernommen werden.

P 17 Ein Benutzerkonzept für das Rechnungswesen war zum Zeitpunkt der Prüfung nicht in Kraft. Dessen ungeachtet wurden Benutzerrechte eingerichtet und produktiv umgesetzt.

P 18 Eine Funktionstrennung ist derzeit nicht realisiert.

Protokollanmerkung: wird zukünftig durch in KSM realisiert

P 19 Aus der Finanzdienstanweisung zur Organisation des Rechnungswesens vom 01.01.2018 in der Fassung vom 12.04.2018 konnten keine Festlegungen über den Umgang mit elektronisch eingehenden originären Rechnungsbelegen im PDF-Format und der Rechnungsverarbeitung entnommen werden.

P 20 Es wurde gegen die Finanzdienstanweisung zur Organisation des Rechnungswesens vom 01.01.2018 in der Fassung vom 12.04.2018 verstoßen. Die DA zur Organisation des Rechnungswesens ist entsprechend zu ändern.

Protokollanmerkung: wird geändert.

P 21 Es lag seit Doppik-Einführung keine haushaltsrechtliche Freigabe für das Rechnungswesen gemäß § 59 Abs. 2 KV M-V vor.

Protokollanmerkung: siehe P 13

gez. Dittmann/Golnik