STADT GERMERING

**Finanzverwaltung**
Datum 10.10.2023

Beschluss-Vorlage 2023/0399 zur Sitzung am 24.10.2023
des HAUPTAUSSCHUSSES

TOP 7 öffentlich

Betreff: Bericht über die überörtliche Prüfung der Jahresrechnungen und Jahresabschlüsse 2014 bis 2019 durch den Bayer. Kommunalen Prüfungsverband für die Prüfungsgebiete Bauausgaben und allg. Verwaltung
- Stellungnahme der Verwaltung

| Finanzielle Auswirkungen? | Ja | Nein |
|---|---|---|

| Kosten laut Beschlussvorschlag: | Kosten der Gesamtmaßnahme | Folgekosten |
|---|---|---|
| Euro | (nur bei Teilvergaben) | einmalig |
| Kosten lt. Kostenschätzung | | lfd. jährl. |
| Euro | Euro | Euro |

| Veranschlagt im Ergebnis-HH 2023 | im Investitions-HH 2023 | mit Euro | Produktkonto Haushaltsansatz Bereits vergeben |
|---|---|---|---|

| Der zuständige Referent / Die zuständige Referentin wurde gehört | hat zugestimmt | hat nicht zugestimmt |
|---|---|---|

## Sachverhalt:

Über die Grundzüge und Inhalte der Prüfung wurde in der Sitzung des Hauptausschusses am 25.10.2022 berichtet und bereits einzelne Stellungnahmen zur Kenntnis genommen.

Zu folgenden, weiteren Prüfungserinnerungen und Feststellungen des Bayerischen Kommunalen Prüfungsverbandes (Textziffern/TZ) kann eine Stellungnahme durch die zuständigen Ämter erfolgen:

### TZ 17 Restriktive Rechtevergabe in finanzwirksamen Verfahren

Aufgrund der Größenklasse einer Großen Kreisstadt und der damit verbundenen Komplexität sind für die finanzwirksamen Verfahren (z.B. OK.FIS, OK.PWS) dokumentierte Berechtigungskonzepte notwendig, um eine sachgerechte Zugriffsverwaltung zu ermöglichen. Dokumentierte Berechtigungskonzepte lagen zum Zeitpunkt unserer Prüfung nicht vor. Eine detaillierte Prüfung war nicht möglich, da in einem ersten Schritt erst Organisation, Zuständigkeiten, Aufgabenverteilung und Vertretungsregelungen zu ermitteln gewesen wären.

Da den Berechtigungskonzepten in den Anwendungsverfahren im Hinblick auf die Kassensicherheit eine hohe Bedeutung zukommt, wären diese auch für die weiteren finanzwirksamen Verfahren noch zu erstellen.

**a) Unzureichende Funktionstrennung**
Nach § 33 Abs. 1 Nr. 10 KommHV-Doppik sind die Aufgabenbereiche „Administration von Informationssystemen und automatisierten Verfahren“ und die Fach- und Kassenaufgaben gegeneinander abzugrenzen und die dafür Verantwortlichen zu bestimmen; die Aufgaben sollen nicht von demselben Beschäftigten wahrgenommen werden. Gegen eine unzureichende Funktionstrennung bestehen aus Gründen der Kassensicherheit erhebliche Bedenken (zur Funktionstrennung siehe auch Schreml/Bauer/Westner, Kommunales Haushalts- und Wirtschaftsrecht, Erl. zu § 33 KommHV-Doppik i.V. mit Erl. 14 zu § 37 KommHV-Kameralistik).
Die Administration von finanzwirksamen Verfahren wäre außerhalb der Kasse zu organisieren. Die administrativen Rechte für die Beschäftigten der Kasse als auch der Beschäftigten, die mit Kassenabschlussarbeiten betraut sind, wären einzuschränken.

**b) Restriktive Rechtevergabe nach dem Minimalprinzip** Die Zugriffsrechte in den eingesetzten Anwendungsverfahren sollten grundsätzlich von den Aufgaben abhängig sein, die dem Beschäftigten zugewiesen wurden. Dabei sollten immer nur so viele Zugriffsrechte vergeben werden, wie sie für die Wahrnehmung der Aufgaben und die Abwicklung der Geschäftsvorfälle notwendig sind (§ 57 i.V. mit § 33 Abs. 1 Nrn. 3 und 5 KommHV-Doppik sowie Schreml/Bauer/Westner, a.a.O., Erl. zu § 33 KommHV-Doppik i.V. mit VV Nr. 2 zu § 37 KommHV a.F. und Schreml/Bauer/ Westner, a.a.O., Erl. 7 zu § 37 KommHV-Kameralistik; restriktive Rechtevergabe nach dem Minimalprinzip).

**c) Hohe Anzahl administrativer Benutzerkonten**
Wir empfehlen der Stadt, die Notwendigkeit für die hohe Anzahl an administrativen Benutzerkonten im Finanzverfahren zu prüfen. Administrative Rechte sollten möglichst restriktiv vergeben werden.

**d) Pflege von Benutzergruppen und Gruppenmitgliedschaften**
Eine korrekte und effiziente Rechtevergabe basiert idealerweise auf differenziert angelegten und aktuell gepflegten Benutzergruppen und Gruppenmitgliedschaften. Dies erleichtert zum einen die Administration des Verfahrens und minimiert das Risiko einer fehlerhaften Zuweisung von Benutzerrechten. Wir empfehlen, die Zugriffsrechte ausschließlich auf Gruppenebene zu vergeben, um den administrativen Aufwand zur Anpassung der Berechtigungen bei Umsetzungen, Neueinstellungen oder Ausscheiden von Beschäftigten in Grenzen zu halten.

**e) Eingeschränkte personenbezogene Benutzerkonten für sachbearbeitende Verwaltungsaufgaben**
Auch sollten sachbearbeitende Verwaltungsaufgaben nicht mit einem Benutzerkonto, das über umfassende administrative Rechte in den finanzwirksamen Verfahren verfügt, erledigt werden. Hierfür sollte aus Gründen der Verfahrens- und Kassensicherheit ein eigenes (personenbezogenes) Benutzerkonto mit nur eingeschränkten Rechten verwendet werden.

**f) Verwendung sicherer Passwörter und zeitnahe Deaktivierung von Benutzerkonten ausgeschiedener Beschäftigter**
Nach Möglichkeit sollten in jedem Fachverfahren die Anforderungen an die Mindesteigenschaten der Kennwörter sowie eine automatisierte Sperrung der Benutzerzugänge nach fehlerhaften Anmeldeversuchen definiert und die Beschäftigten zur Verwendung von sicheren Passwörtern

angehalten werden (vgl. die Basis-Anforderung ORP.4.A23 „Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme“ des BSI-Kompendiums).
Zudem wären die Benutzerkonten für ausgeschiedene Beschäftigte zeitnah zu deaktivieren.

Zu Buchstaben a) bis f):
Eine differenzierte und restriktive Rechtevergabe wäre in allen finanzwirksamen Verfahren umzusetzen. Wir empfehlen, sich bezüglich der Umsetzung eines geeigneten Berechtigungskonzeptes mit den Verfahrensanbietern abzustimmen.

*Die Stadtkämmerei nimmt dazu wie folgt Stellung:*

Aktuell wird ein Berechtigungskonzept für OK-FIS erstellt. Dies wird dahingehend aufgebaut, dass jede/r Mitarbeiter/in mit seinem/ihrem Login nur diejenigen Daten/Informationen bearbeiten bzw. sehen kann die in seinem/ihrem Zuständigkeitsbereich liegen. Dies betrifft die ständigen Tätigkeiten als auch die vertretenden Tätigkeiten.
Die Berechtigungen werden dabei nicht mehr den einzelnen Usern direkt zugewiesen, sondern jeder User bekommt eine oder mehrere, noch in OK-FIS anzulegende, Rollen zugewiesen.

Die Vorlage der Ausarbeitung des Rollenkonzeptes wird in einer der nächsten Sitzungen des Hauptausschusses vorgelegt werden.

**Vorschlag zum Beschluss:**
Der Hauptausschuss nimmt die Ausführungen zu der Ziffer 17 im allgemeinen überörtlichen Prüfbericht der Verwaltung zur Kenntnis.

Mirjam Wolf - Markus Sperber - René Mroncz genehmigt OB