gpa Baden-Württemberg
Kommunale Prüfung und Beratung

GPA-Mitteilung 8/2006

Az. 049.05

01.12.2006

Berechtigungsvergabe bei Einsatz von ADV-Verfahren hier: Trennung von Verantwortungsbereichen

1 Vorbemerkung

Zugriffe auf Programme und Anwendungsdaten können unterschiedliche Auswirkungen haben. Dabei ist zu unterscheiden zwischen beabsichtigten Verarbeitungsergebnissen einerseits (z.B. bewusste Änderung eines Datensatzes) und ungewollten Programmzuständen andererseits. Zu Letzteren gehören nicht nur die Manipulation an Programmen und Anwendungsdaten, sondern z. B. auch schlechtes Laufzeitverhalten durch fehlerhaftes Programmhandling, Systemabstürze oder Dateninkonsistenzen (sog. Datenschiefstände).

Die Auswirkungen von Zugriffen können außerdem unterschiedliche Reichweiten haben:

- systemweit/mandantenübergreifend (anwenderübergreifend),
- mandantenweit/einzelfallübergreifend oder
- auf einen einzelnen Datensatz (Einzelfall) bezogen.

Die Vergabe von Zugriffsberechtigungen ist deshalb restriktiv und an folgenden Zielen ausgerichtet zu erteilen:

- Ordnungsgemäßer und sachgerechter Umgang mit den durch das Programm verwalteten (öffentlichen) Mitteln und darauf aufbauend eine
- anzustrebende hohe Daten- und Ablaufsicherheit.

Gemeindeprüfungsanstalt Baden-Württemberg
76133 Karlsruhe · Hoffstraße. 1a · Telefon 0721 / 8 50 05 - 0
70193 Stuttgart · Klopstockstraße 35 · Telefon 0711 / 6 36 71 - 0

Um dies zu erreichen, müssen die Verantwortungsbereiche der Programmierung, der DV-Administration und der (Einzelfall-)Sachbearbeitung getrennt werden. Zudem sind Trennungen innerhalb dieser Bereiche angebracht. Beispiele:

- Trennung von Feststellung und Anordnung sowie Anordnung und Vollzug auf der Sachbearbeiterebene[1],
- Trennung in allgemeine administrative Tätigkeiten (z.B. Rechnersteuerung, Datensicherung) und verfahrensspezifische Tätigkeiten (z.B. Betreuung eines ADV-Verfahrens),
- Trennung von Programmentwicklung und -transport (in das Produktivsystem).[2]

Zu beachten ist außerdem, dass sich die konkrete Trennung von Verantwortungsbereichen auch an der jeweiligen DV-Struktur auszurichten hat. Beispiele:

- Großrechner- oder Client-Serverumgebung bzw. Stand-alone-Lösung,
- Autonome Lösung (eine Kommune betreibt ihr „eigenes Rechenzentrum“) oder Rechenzentrumslösung,
- Nutzung der Möglichkeiten einer Fernwartung (in diesem Fall können Dritte auf das DV-System zugreifen).

Eine ordnungsgemäße Verarbeitung der Daten setzt voraus, dass der Zugriffsberechtigte (Programmierer, Administrator, Sachbearbeiter) in der Lage ist, die Auswirkungen seines Eingriffs auf die Systemstruktur und das Systemverhalten einzuschätzen. Vor Erteilung einer Zugriffsberechtigung ist deshalb dem (künftigen) Zugriffsberechtigten die aufgabenbezogene Sachkenntnis und Kompetenz für den jeweiligen Programmeingriff ggf. durch geeignete Maßnahmen zu vermitteln.

Nachfolgend werden auf Basis einer Rechenzentrumslösung die unterschiedlichen Programmzugriffe beispielhaft[3] katalogisiert beschrieben. Setzt eine Gemeinde ein autonomes ADV-Verfahren auf einer eigenen DV-Anlage ein, so gelten die nachfolgenden Ausführungen entsprechend mit der Maßgabe, dass an Stelle des (Regionalen) Rechenzentrums die eigene IuK-Abteilung tritt.

---

[1] § 6 Abs. 2 Satz 2 und Abs. 3 GemKVO.

[2] Die Thematik der Programmierung wird hier nicht näher betrachtet.

[3] Auch bei einer Rechenzentrumslösung sind die möglichen Ausprägungen vielfältig, sodass die nachfolgenden Ausführungen lediglich eine Möglichkeit darstellen.

2 Kategorien von Zugriffsberechtigungen

2.1 Sachbearbeitung beim Anwender vor Ort

- Datenermittlung, -erfassung und -eingabe im Einzelfall (z.B. Erfassen eines Personalfalls),
- Vorgangsbezogene Tätigkeiten im Aufgabenbereich des Mitarbeiters (z.B. Durchführen von Zahlläufen durch die Kasse).

Die Dateneingaben wirken sich **einzelfall- bzw. vorgangsbezogen** aus. Bei Fehlern ist der einzelne Datensatz (bzw. sind die durch den Vorgang berührten Datensätze) betroffen. Der Sachbearbeiter muss die aufgaben- und verfahrensbezogene Sachkenntnis und Kompetenz aufweisen.

Die Zugriffsberechtigungen müssen die aufgabenbezogenen Anforderungen an die Trennung von Verantwortungsbereichen erfüllen (z.B. **Trennung von Feststellung und Anordnung**, **Trennung von Anordnung und Vollzug**).

2.2 Administration beim Anwender vor Ort

2.2.1 Verfahrensbezogene Administration (Fachamt bzw. IuK-Abteilung)

- Individuelle Anpassung von Standardsoftware (Customizing),
- Einzelfallübergreifende Datenermittlung, -erfassung und -eingabe (z.B. Stammdaten zur Parametrierung),
- Definition von individuellen verfahrensbezogenen Benutzerrechten; Zuordnung von Benutzern zu den Benutzerrechten und deren Dokumentation,
- Mandantenbezogene Massendatenverarbeitungen ohne Einzelfallbezug (z.B. Weiterleiten von Dateien für den Datenträgeraustausch).

2.2.2

Allgemeine Administration (z.B. IuK-Abteilung)

- Betreuung der Soft- und Hardwarekomponenten vor Ort im Rahmen der allgemeinen DV-Administration,
- Verfahrensunabhängige Berechtigungsverwaltung (z.B. Betriebssystemebene der Arbeitsplatz-PC),
- Verfahrensunabhängige Datensicherung und -archivierung.

Diese Abläufe sind dadurch gekennzeichnet, dass sie sich auf **Mandantenebene** auswirken. Das Risikopotenzial ist höher als unter Abschn. 2.1. Bei Fehlern kann der gesamte Datenbestand des Mandanten (des Anwenders) betroffen sein (z.B. durch fehlerhaftes individuelles Customizing). Die teilweise sehr systemnahe Sachkenntnis und Kompetenz für den jeweiligen Programmeingriff liegt beim entsprechend geschulten Administrator, der das Bindeglied zwischen der (Einzelfall-)Sachbearbeitung (Abschn. 2.1) und dem Rechenzentrum (Abschn. 2.3) darstellt.

Bei der Vergabe der Zugriffsberechtigungen ist insbesondere auf eine **ausreichende Trennung der Tätigkeitsbereiche der Administration und der fachlichen Sachbearbeitung (einschließlich der Erledigung von Kassenaufgaben)** zu achten. Insbesondere darf durch die Vergabe von „administrativen Zugriffsrechten" die Trennung von Verantwortungsbereichen nach Abschn. 2.1 (z.B. die Trennung von Anordnung und Vollzug) nicht aufgehoben werden.

2.3 (Regionales) Rechenzentrum

2.3.1 Verfahrensbezogene Administration (für einzelne Fachanwendungen)

- Allgemeine Anpassung von Standardsoftware (Customizing),
- Strukturierung der Berechtigungsverwaltung mit Blick auf das Fachverfahren als Ganzes (z.B. Definition von allgemein verwendbaren Benutzergruppen und Benutzerrechten),
- Mandantenübergreifende Massendatenverarbeitung (z.B. Realisierung des elektronischen Datenaustausches mit Behörden).

2.3.2 Allgemeine DV-Administration (bezogen auf den Rechenzentrumsbetrieb)

- Konfigurieren und Bedienen aller Einheiten des Datenverarbeitungssystems (Großrechner, Server, Netze usw.),
- Strukturieren der Berechtigungsverwaltung mit Blick auf das DV-System als Ganzes.

Diese Handlungen sowie evtl. Fehler wirken sich (i.d.R.) **systemweit** aus. Das Risikopotenzial ist insoweit hoch einzuschätzen. Dementsprechend ist eine hohe dv-bezogene Sachkenntnis und Kompetenz für diese Eingriffe erforderlich. Die obigen Handlungen dürfen deshalb **nur von den Mitarbeitern des Rechenzentrums** ausgeführt werden.

2.4 Gesamtsicht

Die einzurichtenden anwendungsbezogenen Zugriffsberechtigungen können mit folgendem Raster grob zugeordnet werden:

	Reichweite			
Parameter	**systemweit/mandantenweit**		**mandantenweit**	
	allgemeine Steuerungsdaten	**Rechenzentrum**	individuelle Steuerungsdaten	**Administration (vor Ort)**
Datensätze	**vorgangs- bzw. einzelfallbezogen**			
	Stammdaten	**Sachbearbeitung**	Bewegungsdaten	**Sachbearbeitung**

3 Überschneidung von Verantwortungsbereichen

3.1 Ausgangslage

Das Regionale Rechenzentrum wird für die Gemeinde als sog. andere (öffentliche) Stelle i.S. der VwV-GemKVO unter folgenden Rahmenbedingungen tätig:[1]

- Nach Nr. 4 zu § 1 VwV-GemKVO bleibt der Anwender, explizit die Gemeindekasse, auch dann für die Erledigung der Kassengeschäfte und der anderen Aufgaben verantwortlich, wenn er sich hierbei der EDV-Anlage einer solchen anderen Stelle bedient.[2]
- Die Richtigkeit und Vollständigkeit der Datenerfassung, -eingabe, -verarbeitung, -speicherung und -ausgabe ist sicherzustellen (Nr. 2 zu § 11 VwV-GemKVO). Der Bürgermeister hat dafür zu sorgen, dass die **Einhaltung der erforderlichen Sicherungsvorkehrungen durch diese Stelle** gewährleistet ist.
- Dabei soll sich die Gemeindekasse von der Ordnungsmäßigkeit der erfolgten Eingriffe durch **stichprobenweise Überprüfung der Rechengrundlagen und Rechenergebnisse** überzeugen.

3.2 Problemstellung

Die Komplexität der DV-Systeme bringt es mit sich, dass seitens der Anwender gegenüber dem Rechenzentrum als Dienstleister ein hoher Unterstützungsbedarf artikuliert und angefordert wird. Einerseits wird eine hohe Daten- und Ablaufsicherheit erwartet und vorausgesetzt; andererseits soll das Rechenzentrum aber auch effektiv und effizient Support leisten. Insoweit kommt es zwangsläufig zu einem **Spannungsverhältnis zwischen der Ordnungsmäßigkeit und der Arbeitsfähigkeit des DV-Systems**.

Letztendlich ist es unvermeidlich, dass Mitarbeiter des Rechenzentrums (bzw. Administratoren der eigenen IuK-Abteilung) nicht nur im Rahmen der allgemeinen Administration (Abschn. 2.3.2) auf das DV-System aus systemtechnischer Sicht zugreifen (z.B. Datenbank-

[1] Die VwV-GemKVO ist nach der Bereinigungsanordnung am 31.12.1999 allerdings formal außer Kraft getreten.

[2] Die andere Stelle hat aber der Gemeindekasse gegenüber die Ordnungsmäßigkeit des automatisierten Verfahrens zu bescheinigen (vgl. § 11 Abs. 1 und § 23 Abs. 2 GemKVO, sog. Einsatzbescheinigung).

reorganisation), sondern auch verfahrensbezogen (Abschn. 2.3.1) **im Ausnahmefall** aktive Hilfestellung leisten (z.B. bei der Durchführung einer schwierigen Buchung bzw. bei einer Fehlerbereinigung). In diesem Fall kommt es dann zu einer **Überschneidung der Verantwortungsbereiche des Rechenzentrums** und des **Anwenders**.

3.3 Mögliche Lösungsansätze

Um auch bei einer solchen Überschneidung die erforderliche Sicherheit zu gewährleisten, sind insbesondere folgende Lösungen denkbar.

3.3.1 „Notfall-Lösung“

Im Produktivsystem des kommunalen Anwenders sind - mit Ausnahme eines Notfallbenutzers (o.Ä.) - **keine anwendungsbezogenen Zugriffsrechte** (quasi Sachbearbeiterrechte) für Mitarbeiter des Rechenzentrums angelegt. Dies bedeutet, dass im Falle einer angefragten Unterstützung (z.B. Bereinigung eines Fehlerfalls) eine solche Dienstleistung durch das Rechenzentrum nur stark eingeschränkt erbracht werden kann. Die Aktivierung des Notfallbenutzers erfolgt durch die Mitarbeiter des Rechenzentrums aufgrund schriftlicher Legitimation durch einen Verantwortlichen des Anwenders, wobei ein bestimmtes „Notfallniveau“ erreicht sein muss. Aktivitäten des Notfallbenutzers werden aufgezeichnet.

Hat sich eine Gemeinde (durch den Bürgermeister) für diese Lösung mit einem sehr hohen Maß an Sicherheit entschieden, so hat dieser im Vorfeld von seinem Bestimmungsrecht hinsichtlich der "erforderlichen Sicherungsvorkehrungen" Gebrauch gemacht (vgl. § 23 Abs. 4 Satz 1 GemKVO). Insoweit werden sich die aus der Wahl dieser Variante resultierenden (zusätzlichen) gemeindespezifischen Kontrollen i.d.R. auf die Fälle beschränken können, in denen der "Notfall" eingetreten ist.

3.3.2 Berechtigungsvergabe auf Antrag[1]

Vom Anwender wird über eine User-Help-Desk-Software eine konkrete Hilfestellung beim Rechenzentrum angefordert. Als Antwort erhält er Hinweise zur Problembehebung. Sollten diese Hinweise nicht ausreichend und dennoch ein Zugriff des Rechenzentrums auf das

[1] Nachfolgend wird das Szenario beispielhaft unter Verwendung einer User-Help-Desk-Software beschrieben. Bei solcher Software handelt es sich um ein mit besonderen Funktionalitäten (z.B. der Anzeige des Bearbeitungsstatus, mit Dokumentationsfunktionen usw.) ausgestattetes System, mit dem der Anwender seine Anfrage oder Problemdarstellung an den Support des Rechenzentrums kommunizieren kann.

Kundensystem zur Lösung des Problems notwendig sein, so werden dem zuständigen Mitarbeiter des Rechenzentrums **temporär bis zur Lösung des Problems** Zugriffsrechte für das ADV-System des Anwenders eingeräumt.

Diese Vorgehensweise führt zwar zu mehr Zugriffen durch Rechenzentrums-Mitarbeiter als bei der „Notfall-Lösung“ und damit zu mehr „Risikopotenzial“ und einem höheren Kontrollaufwand. Sie bringt aber auch eine höhere Effizienz durch die zeitnahe Problemlösung mit sich. Gleichzeitig ist sie aber sicherer, als den Rechenzentrums-Mitarbeitern generell Zugriffsrechte einzuräumen (s. dazu Abschn. 3.3.3).

3.3.3 Zugriffe von Mitarbeitern des Rechenzentrums auf Antrag

Hier sind - im Gegensatz zur Variante in Abschn. 3.3.2 - alle mit der Betreuung der Anwender befassten Mitarbeiter des Rechenzentrums mit den für **ihren Aufgabenbereich erforderlichen Berechtigungen** ausgestattet. Diese können u.U. umfassender als die Berechtigungen der Sachbearbeiter vor Ort sein (z.B. Anordnung erfassen und buchen und Zahllauf, Tabellenpflege, Auswertungen, Erfassung und Änderung von Stamm- und Bewegungsdaten). Der **tatsächliche Zugriff** (Eingriff) darf dabei aber **nur auf (schriftlichen) Auftrag des Anwenders** erfolgen. Er muss auf jeden Bedarfsfall bezogen beauftragt werden; Pauschal-Genehmigungen des Anwenders sind nicht zulässig. Allgemeine Aussagen, welchen Umfang die Berechtigungen haben können und dürfen, sind dabei allerdings nicht möglich, sondern müssen sich am Einzelfall ausrichten (z.B. benötigt eine kleinere Gemeinde i.d.R. eine höhere Unterstützungsleistung als eine größere Verwaltung). U.U. ist auch die Anzahl der von einem Rechenzentrum zu betreuenden Anwender zu berücksichtigen; außerdem können im Einzelfall (z.B. bei Releasewechsel, Einführung neuer Verfahrensteile) auch zeitlich begrenzt umfangreiche Zugriffsmöglichkeiten erforderlich sein. Ggf. sollte der Anwender entsprechend seinen individuellen Bedürfnissen den Umfang und die Notwendigkeit der Berechtigungen mit dem Rechenzentrum abklären.

Diese Variante bietet die größte Flexibilität und ist grundsätzlich nicht zu beanstanden, da das Rechenzentrum als sog. andere (öffentliche) Stelle tätig wird (s.o. Abschn. 3.1). Voraussetzung ist, dass sich sowohl die rechenzentrums-, als auch die gemeindespezifischen **organisatorischen und technischen Kontrollen** gezielt auf diese Variante ausrichten. Notwendig sind dabei regelmäßige Kontrollhandlungen auf der Basis von Auswertungen, welche die Zugriffsmöglichkeiten und die tatsächlichen Zugriffe von Mitarbeitern des Rechenzentrums auflisten (z.B. Zeitpunkt des Zugriffs durch Mitarbeiter des Rechenzentrums auf das System, ordnungsgemäße Dokumentation bzw. Protokollierung dieser Zugriffe). Daneben führt diese Variante wegen der Vielzahl der zugelassenen "Nicht-Gemeinde-User" auch

dazu, dass eine Gemeinde die Verarbeitungsergebnisse vermehrt stichprobenweise überprüfen muss. Auch bei dieser Lösung bleibt die Gemeinde für die Erledigung der Aufgaben verantwortlich. Sie muss sich die Verarbeitungsergebnisse in vollem Umfang zurechnen lassen.

SG 41