Kommunalsoftware auf dem Prüfstand[1]

(Auszug aus der Veröffentlichung im OKKSA-Newsletter Nr. 21 vom 18.03.2011)

Teil 10: Haben Stammdaten Jahresringe? Zeitstempel und Historien im Kontext von GoB und Datenschutz (von Dr. Uwe Schwochert).

Einleitung

Die GoB (Grundlagen ordnungsmäßiger Buchführung) und die sich daraus ergebenden Anforderungen an die Revisionsfähigkeit der Datenverarbeitung spielen seitens der OKKSA Kriterien eine zentrale Rolle für den fachübergreifenden Anforderungskatalog. Im nachfolgend betrachteten Kapitel FÜ06 (Kriterien **FÜ06.xx**) wird dabei insbesondere die Protokollierung und Nachverfolgbarkeit von Änderungen an im Programm gespeicherten Daten unter die Lupe genommen. Weitergehend wird betrachtet, wie die entstehenden Protokolldaten insbesondere unter Datenschutzaspekten zu schützen sind.

Zunächst ist festzulegen, bei welchen Daten im Programm entsprechende Mechanismen erforderlich sind. Hier wird eine allgemeine Einteilung nach Stammdaten (zustandsorientiert, längerfristige Speicherung von Sachverhalten – Beispiel: Debitorenkonto, Abgabenhebesatz) und nach Bewegungsdaten (ablauforientiert, widerspiegeln einzelne Ereignisse und entstehen immer wieder neu - Beispiel: Buchung, Bescheiddruck) vorgenommen. In den OKKSA Kriterienkatalogen werden Kriterien, die wichtige Stamm- oder Bewegungsdaten beschreiben, jeweils mit STAMM bzw. BEW gekennzeichnet. Diese Kennzeichnung ist Teil der Diskussion in den entsprechenden Fachgremien.

So entsteht je Fachgebiet eine Liste der zu protokollierenden Daten. Die Anforderungen für diese Protokollierung werden zentral im Kapitel FÜ06 festgelegt.

Protokollierungsanforderungen für Stammdaten

*[**FÜ06.01**] Das Programm überwacht Änderungen der gespeicherten Stammdaten, indem Autor und Zeitpunkt der letzten Veränderung recherchierbar gespeichert werden (**Zeitstempel**). [MUSS-Kriterium]*

Es soll also möglich sein, Veränderungen so zu kennzeichnen, dass keine anonymen oder zeitlich nicht zuordenbaren Korrekturen erfolgen können. Dies setzt einen entsprechend automatisch wirksamem Mechanismus im Programm voraus, wobei hier häufig auf entsprechende Grundfunktionen der verwendeten Datenbankumgebung zugegriffen werden kann. Weiterhin sollen diese Informationen aus der Bearbeitung heraus abrufbar sein, d. h. beim Zugriff auf eine Adresse soll z. B. Herr Schulze erkennen können, dass vor ihm Frau Müller die Adresse zuletzt geändert hat.

Insbesondere bei kritischen Stammdaten sind diese Zeitstempel nicht ausreichend, deshalb wird weitergehend gefordert:

*[**FÜ06.02**] Jeder ändernde Zugriff auf Stammdaten wird über einen längeren Zeitraum verfolgbar feldbezogen protokolliert (**Stammdatenhistorie**). Vorhergehende Inhalte der Datensätze können auch nachträglich eingesehen werden. [KANN-Kriterium]*

[1] Die in der Artikelserie genannten Kriterien stammen aus der aktuellen Version 4.00 des "OKKSA Anforderungskatalogs für Fachprogramme in der Öffentlichen Verwaltung - Teilbereich Fachübergreifende Programmanforderungen (FÜ.B)". Im Kriterienkatalog sind neben den Kriterien auch weitere Rechts- und Normungsgrundlagen genannt, aus denen die genannten Kriterien abgeleitet werden.

*[**FÜ06.02a**] Jeder ändernde Zugriff auf **finanzwirksame** Stammdaten wird über einen längeren Zeitraum verfolgbar feldbezogen protokolliert (**Historie finanz-wirksamer Stammdaten**). Vorhergehende Inhalte der Datensätze können auch nachträglich eingesehen werden. [MUSS-Kriterium]*

Der letzte Satz des Kriteriums (ergänzt bei der aktuellen Überarbeitung des Kriterienkataloges OKKSA FÜ.B zur 4. Ausgabe) stellt klar: es genügt nicht nur ein einfaches Änderungsprotokoll, in dem die Zeitstempel der vorherigen Änderungen des Stammdatums aufgezählt werden, sondern es muss explizit auch die fachliche Änderung selbst gespeichert werden. So sollen z. B. nach der Änderung der Adresse eines Debitors dessen vorherige Adressen immer als "historisierte" Information erkennbar sein.

Diese Anforderung ist nicht zu verwechseln mit der Speicherung zeitraumbezogener Stammdaten. So muss zum Beispiel der Hebesatz für die Grundsteuer oder ein Zinssatz immer zeitraumbezogenen gespeichert werden. Die o. g. Anforderung gilt hier für die Änderung innerhalb eines Zeitraums, wenn also z. B. der Hebesatz für ein Jahr nachträglich geändert wird oder ein Zinssatz für den gleichen Zeitraum angepasst wird.

Selbstverständlich zählt auch die Ersterfassung von Stammdaten als "Änderung", es bedarf also auch hier eines Zeitstempels mit Benutzername.

Eine entsprechende Protokollierung wird zusätzlich explizit auch für die Änderung von Benutzerrechten gefordert (**FÜ04.22** – MUSS).

Ausgehend davon, dass die Änderung eines Stammdatums ein fachlich relevantes Ereignis ist, wird in Kapitel 6 weiterhin gefordert:

*[**FÜ06.03**] Veränderungen von Stammdaten können mit Notizen versehen werden (**Änderungskommentierung**). [KANN-Kriterium]*

Bearbeiter sollen also in der Lage sein, z. B. Gründe für eine Datenänderung oder Verweise auf begründende Unterlagen in einem speziell dafür vorgesehenen Feld einzutragen.

Ein Nebenaspekt der Änderungsprotokollierung, der künftig noch stärker beachtet werden soll, ist die Eintragung künftiger Änderungen. Wenn also z. B. bekannt ist, dass ein Debitor zum 1. des nächsten Monats eine neue Adresse hat, soll dies aktuell erfassbar sein, allerdings soll (1) die neue Adresse erst zum genannten Termin automatisiert verwendet werden und (2) außerdem der Eintrag der neuen Adresse mit Zeitstempel (Zeitpunkt des Eintrags, Benutzername) versehen sein.

Protokollierungsanforderungen für Bewegungsdaten

Bewegungsdaten widerspiegeln einmalige Ereignisse und müssen deshalb im Programm entsprechend geschützt sein. Die Anforderung dazu lautet:

***[FÜ06.04]** Das Programm verhindert, dass Bewegungsdaten nachträglich geändert oder gelöscht werden. Entstehungszeitpunkt und Autor sind gespeichert und im Nachhinein erkennbar (**Bewegungsdatenzeitstempel**).*

Neben dem Zeitstempel muss also programmtechnisch auch sichergestellt sein, dass Bewegungsdaten nachträglich nicht gelöscht werden können. Eine entsprechende Kenn-

zeichnung erfolgt in den OKKSA Kriterienkatalogen bei allen fachlich relevanten Bewegungsdaten. Denn die Information über einen erzeugten Bescheid, eine Buchung, einen Abschluss oder eine gelegte Rechnung widerspiegelt ein fachlich relevantes Ereignis, entsprechend den GoB darf die Information darüber nicht nachträglich verändert werden.

Dabei ist zwischen der fachlichen Information ("Rechnung wurde mit einem bestimmten Inhalt erstellt") und technischen Hilfsinformationen (z. B. eine binäre Druckdatei, wie sie zum Ausdruck an den jeweiligen Drucker geschickt wurde) zu unterscheiden. Der Bewegungsdatenschutz bezieht sich auf die fachliche Information zum Sachverhalt, die Binärdatei ist eher ein Thema für die Archivierung.

Praktische Probleme

Sowohl die Protokollierung von Stammdaten als auch der Schutz der Bewegungsdaten scheitern in der Praxis regelmäßig an technisch bedingten Umstellungs- und Fehlersituationen. Sobald z. B. ein Finanzprogramm gewechselt wird und Daten von einem in ein anderes Programm konvertiert werden, entstehen meist auch neue Zeitstempel. Genau genommen erfolgt, zumindest aus technischer Sicht, auch eine Änderung der Informationen.

Eine Umsetzung der o. g. Anforderungen würde in dieser Situation bedeuten, dass immer auch die Historie mit sämtlichen Zeitstempeln der Stammdaten Teil der Konvertierung sind. Bei den Bewegungsdaten wäre zusätzlich durch geeignete Überwachungsroutinen sicher zu stellen, dass sie vollständig übernommen werden, was z. B. die Nutzung einer programmübergreifenden und kontrollierbaren Nummerierungsbasis (z. B. fortlaufende Bescheidnummer) voraussetzt.

Es wird deutlich, dass eine abschließende Klärung der sich ergebenden Anforderungen an die Programmunterstützung an dieser Stelle nicht möglich ist. Zunächst ist jedoch wichtig, dass sowohl beim Programmwechsel als auch im Fehler- und Datenwiederherstellungsfall ein entsprechend sorgfältiges Vorgehen und ein Wissen um die programminternen Protokollierungsmechanismen erforderlich sind.

Sicherung der Änderungsprotokolle

Betrachtet man die Vielzahl an Stamm- und Bewegungsdaten, die bei einem hinreichend komplexen Fachverfahren anfallen, so wird schnell deutlich, dass hier ein großes Volumen an personenbezogenen Protokollinformationen entsteht. Genau genommen entstehen diese Informationen heute in fast jedem hinreichend qualifizierten Datenhaltungssystem, so z. B. auch beim Betrieb eines Servers, wo zu jeder Datei Zugriffe, Änderungsinformationen und auch historische Versionen (Sicherungskopien) gespeichert werden.

Diese Informationen sind im Einzelfall unkritisch, wenn es also darum geht, wer wann zuletzt eine Datei gespeichert oder eine Adresse geändert hat.

Werden diese Informationen jedoch insgesamt und personenorientiert ausgewertet, entstehen Personenprofile, die unter Datenschutzaspekten als kritisch einzustufen sind. So könnten Rückschlüsse auf Arbeits- und Pausenzeiten, Arbeitsintensität oder Fehlerhäufigkeit eines einzelnen Mitarbeiters gezogen werden.

Mit der 4. Ausgabe des Kriterienkataloges OKKSA FÜ.B wurden diese Aspekte erstmals in Form von drei Programmanforderungen berücksichtigt. Die neuen Kriterien werden dabei

als erster Schritt gesehen, eine künftige Präzisierung und Verschärfung der Anforderungen ist vorgesehen.

[FÜ06.05] *Das Programm ermöglicht die Einstellung differenzierter Zugriffsrestriktionen für die systematische Auswertung und Löschung der im Rahmen der Datenprotokollierung anfallenden Informationen. [MUSS-Kriterium]*

Mit diesem Kriterium wird explizit formuliert, dass die bei der Protokollierung entstehenden Informationen, wenn sie systematisch ausgewertet oder gelöscht werden sollen, schützenswerte Objekte des Zugriffschutzes sind. Es geht hier also nicht um den fachlich erforderlichen Einzelzugriff, welcher normalerweise mit den gleichen Zugriffsrechten erfolgt, wie auch der Zugriff auf das jeweilige Stamm- oder Bewegungsdatum selbst. Vielmehr wird hier der eher aus administrativen Gründen erforderliche Gesamtzugriff auf die Protokollinformationen betrachtet.

Weiterhin gilt, dass eine nachträglich mögliche Veränderung dem Sinn der Datenprotokollierung entgegenstehen würde:

[FÜ06.06] *Das Programm verhindert die nachträgliche Veränderung der im Rahmen der Datenprotokollierung anfallenden Informationen. [KANN-Kriterium]*

Mittelfristig, sobald sich in der Praxis eine sichere Umsetzungsform dieses Protokollschutzes abzeichnet, ist an dieser Stelle eine Verschärfung des Kriteriums auf MUSS zu erwarten.

Unter Datenschutzaspekten ist eine regelmäßige Löschung der entstandenen Protokollinformationen erforderlich. Dies wird momentan noch als größtes Problem gesehen, da eine Separierung löschenswerter und nicht zu löschender Informationen äußerst schwierig ist.

Zunächst besteht jedoch die Anforderung, dass es überhaupt eine Möglichkeit gibt, die entstandenen Protokollinformationen zu löschen:

[FÜ06.07] *Das Programm unterstützt die zeitraumbezogene Löschung historisierter bzw. protokollierter Informationen. [KANN-Kriterium]*

Auch dieses neue Kriterium greift relativ weit und ist deshalb zunächst mit KANN gewichtet. Hier kann der Programmentwickler kaum auf Mechanismen der Betriebssystem- oder Entwicklungsumgebung zurückgreifen. Dieses Problem betrifft weitergehend ja auch Betriebssysteme wie Microsoft Windows mit den im Dateisystem verankerten Zeitstempeln.

OKKSA strebt an, dass künftig zusammen mit Datenschützern hier einheitliche Vorgaben entwickelt werden. Diese sollten um Umsetzungshinweise hinsichtlich der verbreiteten Datenbank- und Betriebssystemumgebungen ergänzt werden.

Nächster Teil der Serie: Zuverlässigkeit, Datensicherung, Service: Wer kann das überprüfen?