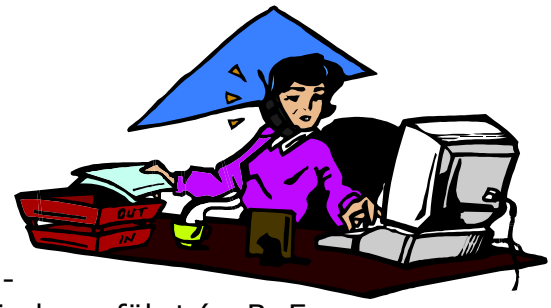
Artikelserie "Programme auf dem Prüfstand"
(Auszug aus der Veröffentlichung im OKKSA-Newsletter Nr. 25)

Teil 14: Was muss ein Programm über sich verraten?

(von Dr. Uwe Schwochert)



Klarheit für den Benutzer

Wer weiß heute eigentlich noch, mit welcher Office-Version er arbeitet, welches Windows und welchen Prozessortyp er einsetzt? Vielleicht sind das auch nicht wirklich die entscheidenden Fragen. Wenn jedoch das Programm fachspezifische Vorgänge weitestgehend automatisch ausführt (z. B. Erzeugen von Abgabenbescheiden) müssen wir uns auf seine Korrektheit verlassen können. Und dieses Verlassen beginnt genau genommen damit, dass wir wissen, mit welchem Programm wir arbeiten.

Um das zu gewährleisten, wird im Kriterienkatalog FÜ.B gefordert, dass jedes fachspezifisch eingesetzte Programm diese Informationen bei seiner Benutzung bereitstellt:

> [**FÜ08.07**] Bei der Nutzung des Programms sind folgende Angaben für den Programmbenutzer erkennbar beziehungsweise abrufbar:
> 1. **Name** des Programms beziehungsweise Programmteiles,
> 2. **Versionsnummer**,
> 3. **Releasestand** (Datumsangabe).
>
> [MUSS-Kriterium]

Übliche Orte für diese Informationen sind z. B. der Startbildschirm, die Statusleiste oder ein entsprechender Menüpunkt. Wichtig ist, dass diese Informationen z. B. im Supportfall unkompliziert und schnell durch jeden Programmbenutzer erreichbar sind.

Entsprechende Informationen sind auch bei fachbezogen genutzten Cloud-Lösungen erforderlich.

Neben den im Kriterium genannten Punkten sind je nach Herkunft, Struktur und Anwendungskontext weitere Informationen erforderlich. So könnte die Information im genannten Fall eines Programms zur Erzeugung von Abgabenbescheiden wie folgt aussehen:

> **Fixfinanz plus Großstadt-Edition**
> Enthalten: Modul Grundsteuer, Modul Bescheiderstellung
> Version 4.3 Patch 44856, Release 28.02.2015
>
> Lizenziert für Stadtverwaltung Musterstedt
> © Fix-Software
>
> Verwendete Bibliotheken:
> ManagedFinanzCodeLibrary © Fix-Software 2005, PrintFixLibrary © NOSoftware 2011

Die genaue Art der Programmversionierung und auch die an dieser Stelle notwendige Form der Darstellung ist letztlich Sache des Programmentwicklers. Eine Grundanforderung, gerade auch hinsichtlich des prüfbaren Programmeinsatzes, ist jedoch, dass mit der Deklaration von Versionierung und Modulabgrenzung eine eindeutige Anwendungssituation entsteht. Das bedeutet:

1. Die hier angegebene Programmversion soll eindeutig den aktuellen Entwicklungsstand

repräsentieren. Eine zu "grobe" Angabe, z. B. der Hauptversion (also "Fixfinanz plus Reihe 4") genügt nicht, wenn es innerhalb dieser Reihe Programmänderungen gibt, die für den Anwender relevant sind. Eine sehr granulare Angabe (z. B. Patchnummer) ist jedoch i. d. R. kein Problem, sofern sich damit ein eindeutiger Bezug zu einem dokumentierten Releasestand herstellen lässt.

2. Für den Anwender soll erkennbar sein, wenn er organisationsspezifische Anpassungen der Programmfunktionalität nutzt. Dies meint zum Beispiel eine Anpassungsprogrammierung (Customizing), die auf die Anwenderorganisation zugeschnitten ist und die über die programmseitig vorgesehenen Einstellungen (Einstellungsdialog, Druckformulare) hinausgeht. Ggf. unterliegen diese Anpassungen einer eigenen Versionierung.

3. Das genutzte Programm soll eindeutig abgrenzbar sein, damit zum Beispiel der Einsatz von speziellen, nicht zum Standard gehörenden Modulen erkennbar ist. Je nachdem, wie die Module des Programms entwickelt, ausgeliefert und dokumentiert werden, sind die Einzelversionen der eingesetzten Programmmodule anzugeben.

Deklaration der Programmweiterentwicklung

Im Verlauf der Zeit genügt für eine verbindliche und rechtskonforme Programmbenutzung nicht nur die einmalige Angabe der o. g. Identifikationsdaten. Da sich der Benutzer auf die Programmfunktionalität verlassen muss, muss er auch die Möglichkeit haben, sich über deren Weiterentwicklung zu informieren. Dazu gehören

1. Informationen darüber, dass ein **neues Programmrelease** eingespielt wird (zum Beispiel über den Herstellerservice oder automatisch per Internet).
2. Informationen darüber, welche für den Anwender **relevanten Programmänderungen** mit dem Releasewechsel verbunden sind.

Die Anforderung im Kriterienkatalog FÜ.B dazu lautet:

> [**FÜ08.08**] Die **Änderung des Standes des Programms** wird dem Anwender bei der Programmbenutzung explizit kenntlich gemacht.
> [KANN-Kriterium]

Die Information über das neue Release soll also "bemerkbar" sein, eine bloße Änderung der Programminformationen (die z. B. über einen Menüpunkt aufgerufen werden müssen) genügt nicht. Üblich sind z. B. einmalige Informationsfenster, die beim Programmstart erscheinen und einen Link auf die Release-Notes enthalten.

Da es hier um (rechts-)verbindlich eingesetzte und in der Regel prüfpflichtige Programme geht, sollten die Informationen zu den vorgenommenen Releaseänderungen vorab bereitstehen, um ggf. notwendige Änderungen der Programmnutzung einzuleiten. Dazu empfiehlt sich die Einrichtung einer zuständigen Stelle in jeder das Programm nutzenden Fachabteilung. Diese sollte je nach Umfang der Programmänderungen die Möglichkeit erhalten, das neue Release vor dem Einsatz zu testen.

Allerdings entbindet die Existenz einer zuständigen (Freigabe-) Stelle in der Anwenderorganisation nicht davon, dass die das Programm verantwortlich einsetzenden Anwender ebenfalls über die Programmänderung informiert werden müssen.

Verfahrensverzeichnis

Entsprechend den Landesdatenschutzgesetzen sind öffentliche Stellen zur Führung eines Verfahrensverzeichnisses verpflichtet. So lautet § 7 Abs. 1 LDSG Schleswig-Holstein:

```
(1) Die datenverarbeitende Stelle erstellt für jedes von ihr betriebene automatisierte Verfahren ein Verfahrensverzeichnis. Dieses Verzeichnis kann auch von einer Stelle für andere geführt werden. Es enthält Angaben über
1. Name und Anschrift der datenverarbeitenden Stelle,
2. Zweckbestimmung und Rechtsgrundlage des Verfahrens,
```



```
3. den Kreis der Betroffenen,
4. die Kategorien der verarbeiteten Daten und deren Aufbewahrungs- oder Löschfris-
ten
5. die Personen und Stellen, die Daten erhalten oder erhalten dürfen einschließlich
der Auftragnehmenden,
6. geplante Datenübermittlungen an Stellen außerhalb der Mitgliedstaaten der Euro-
päischen Union,
7. die datenschutzrechtliche Beurteilung der oder des behördlichen Datenschutzbe-
auftragten, soweit eine solche vorliegt,
8. eine allgemeine Beschreibung der nach den §§ 5 und 6 zur Einhaltung der Datensi-
cherheit getroffenen Maßnahmen.
```

Hier geht es zunächst um eine Anforderung an die einsetzende Stelle des Programms. Dabei ergeben sich allerdings zwei wichtige Aspekte:

1. Die meisten der genannten Informationen sind beim fachspezifischen Programmeinsatz **nicht spezifisch für die einsetzende Organisation** sondern eher für das eingesetzte Programm. Entsprechend ist es wesentlich effizienter, wenn diese Informationen (z. B. Rechtsgrundlage der Datenverarbeitung, Datenübermittlungen) der Programmdokumentation "ab Werk" beigefügt werden. Nicht zuletzt muss sich auch der Programmentwickler vorab genau damit auseinandersetzen. Vor dem Hintergrund der Programmprüfung betrifft diese Auseinandersetzung auch Punkte wie z. B. die datenschutzrechtliche Beurteilung (insbesondere bei neuen Datenverarbeitungskonzepten ist der Anbieter angehalten, diese vorab einzuholen) oder die Datensicherheit (auch dafür sollte das Programm ab Werk konzeptionell ausreichend gerüstet sein).
2. Detailinformationen zum Umfang der gespeicherten Daten (und auch ihrer Adressaten) liegen im Zweifelsfall **nur beim Programmentwickler in einer ausreichenden Qualität** vor.
   Der (neue) Programmanwender und auch der externe Prüfer können in Anbetracht komplexer und oft unzureichend dokumentierter Datenmodelle moderner Fachverfahren nur schwer den tatsächlichen Umfang der vorgesehenen Datenspeicherung und –verarbeitung beurteilen. Denn dieser definiert sich in erster Line aus den vorhandenen Speicher- und Verarbeitungsfunktionen des Programms.
   Letztlich kann das zu führende Verfahrensverzeichnis nur dann einen rechtskonformen Zustand dokumentieren, wenn Datenschutz-Konformität bereits bei der Programmentwicklung eine Rolle spielte.

Aus diesen beiden Gründen ergibt sich die große Bedeutung von "Zuarbeiten" der Programmentwickler für das Verfahrensverzeichnis. Das entsprechende Kriterium lautet:

[**FÜ08.09**] Das Programm oder die Programmdokumentation unterstützt die Beschaffung und Verwaltung folgender für die Erstellung des **Verfahrensverzeichnisses** notwendigen Informationen:

1. Name des eingesetzten Programms,
2. Zweckbestimmung und Rechtsgrundlage des Programms,
3. Kreis der Betroffenen,
4. zugriffsberechtigte Personen.

[KANN-Kriterium]

Sicherheitsdokumentation

Ähnlich wie mit dem programmbezogenen Datenschutz verhält es sich mit dem sicheren Einsatz des Programms. Viele Aspekte des sicheren Einsatzes ergeben sich direkt aus der Konzeption des eingesetzten Programms und seiner Sicherheitsmerkmale. Entsprechend sollte bereits bei seiner Entwicklung das Konzept des sicheren Einsatzes in einer Anwenderorganisation berücksichtigt werden. Dazu gehören u. a.:

1. Einsatz sicherer Übertragungstechnologien für die Datenübermittlung (auch bei Webanwendung),
2. Verschlüsselungstechnologien für die Sicherung von Datenträgern,

3. Einsatz sicherheitsgeprüfter Rechenzentren für Hosting-Dienste,
4. Sicherheitsmerkmale des Benutzerzugangs zu den Programmdaten.

Aus den vorab zu definierenden Konzepten ergeben sich Maßgaben für die Organisation eines sicheren Programmeinsatzes in der Anwenderorganisation.

Mit dem folgenden Kriterium werden diese Maßgaben "ab Werk" eingefordert:

[**FÜ08.10**] Die Programmdokumentation enthält programmspezifische Hinweise, mit welchen Maßnahmen beim Betrieb des Programms die Sicherheit der damit verbundenen IT-Systeme und IT-Anwendungen gewährleistet werden kann. (**Sicherheitsdokumentation**)
[KANN-Kriterium]

Der Darlegung der empfohlenen Sicherheitsmaßnahmen sollte eine dokumentierte Risikobetrachtung zu Grunde liegen.

Für den Fall einer Nutzung des Programms über das Internet (Cloud-Lösung) wird diese Anforderung im Kriterium FÜ11.01 weiter spezifiziert und zum MUSS-Kriterium.

Weitergehende Unterstützung der Einsatzkonzeption

Mit den vorgenannten Kriterien wird eine Unterstützung des sicheren und rechtsverbindlichen Programmeinsatzes gefordert. Dieses Thema wird mit dem aktuellen Kriterienkatalog OKKSA FÜ.B (auch unter Berücksichtigung der bereits diskutierten Dokumentationsanforderungen) jedoch nicht ausgeschöpft. Weitere, im Rahmen von Ausschreibungsverfahren abzufragende Aspekte könnten sein:

- Benennung von Normen und Standards, zu denen das Programm nachweislich konform ist.
- Benennung der vorgesehenen Möglichkeiten, wie der Anwender Einfluss auf die Weiterentwicklung des Programms nehmen kann (Ansprechpartner, Internet-Forum, OKKSA-Fachgremium, ...).
- Benennung der anwenderseitig erforderlichen Schulungen und Einweisungen in Abhängigkeit von Vorkenntnissen.
- Bereitstellung eines Migrationskonzeptes bzw. Musterablaufes zum Übergang von einem Vorgängerverfahren.
- Bereitstellung von Modellen der seitens des Programms implizierten Arbeitsabläufe beim Anwender.
- Ergänzung der Sicherheitsdokumentation um
  - Auflistung eingesetzter sicherheitskritischer Technologien (wie z. B. Flash),
  - Auflistung von hinsichtlich der Rechenzentrumsverarbeitung bestehenden Unterauftragsverhältnissen,
  - Auflistung von hinsichtlich Entwicklung und Support bestehenden Unterauftragsverhältnissen,
  - Vorschläge zur zusätzlichen Erhöhung der Verarbeitungssicherheit (z. B. Verschlüsselung Datenträger, spezielle Trennung von Zugriffsrechten).

Hinweis: Die in der Artikelserie genannten Kriterien stammen aus der aktuellen 4. Ausgabe 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.

Nächster Teil der Serie:
Programmschnittstellen – Konnektivität unter der Lupe

