

Anforderungskatalog für Fachprogramme in der Öffentlichen Verwaltung

Teilbereich:

Fachübergreifende Programmanforderungen (Kriterien OKKSA FÜ.B)

Impressum

Anforderungskatalog für Fachprogramme in der Öffentlichen Verwaltung

Teilbereich: Fachübergreifende Programmanforderungen
Katalogkürzel: FÜ.B
Ausgabe: 5
Version: 5.03
Stand: 16.11.2016
Herausgeber:



Redaktion: OKKSA e. V., www.okksa.de
Herr Dr.-Ing. Uwe Schwochert
Halankweg 15
01156 Dresden
Tel. 0351 / 4163820
Fax 0351 / 4163819
E-Mail: schwochert@trustbit.de
Fachgremium: OKKSA-Center FÜ.B (s. Absatz 2.3)
Internet: www.okksa.de/fachgebiete/fue_b
Freigabe: 15.11.2016
gültig bis: 30.11.2019 (Verlängerungen dazu siehe www.okksa.de/fachgebiete/)

Die Erstellung dieses Anforderungskataloges wurde unterstützt durch:

TRUSTBIT

TRUSTBIT Prüfstelle für Fachprogramme

www.trustbit.de

Allgemeiner Hinweis: Der Anforderungskatalog ist trotz seiner engen Bezüge zu rechtlichen Bestimmungen lediglich eine prüffähige Dokumentation eines fachlichen Abstimmungsprozesses, die keine Garantie für Vollständigkeit und abschließende Behandlung des Themas beinhaltet. Er beinhaltet Anforderungen an IT-Lösungen, die eine rechtskonforme Bearbeitung der regelmäßig anfallenden Vorgänge der laufenden Verwaltung im betreffenden Teilbereich ermöglichen sollen, nicht Anforderungen an konkretes Verwaltungshandeln selbst bzw. an Nutzungskonzeptionen von entsprechenden IT-Lösungen.

Das vorliegende Dokument ist keine von öffentlicher oder gesetzgeberischer Seite legitimierte Rechts- oder Handlungsgrundlage (auch wenn rechtliche Grundlagen möglichst genau abgebildet werden sollten). Für die Verwendung der Kriterien und der nach diesen Kriterien geprüften Programme und Systeme kann keine Garantie übernommen werden.

Nutzungshinweis: Der (freigegebene) Anforderungskatalog kann durch Softwareentwickler und -anwender zur Betrachtung ihrer jeweiligen Produkte und Anwendungssituationen verwendet werden. Die Nutzung für die Erbringung von Dienstleistungen gegenüber Dritten und die sonstige Verwertung bedarf der Genehmigung des jeweiligen Redakteurs.

Anforderungskataloge können über die Website des OKKSA-Vereins (www.okksa.de) bestellt werden. Eine Weitergabe an Dritte ist nicht gestattet.

Inhaltsverzeichnis

1. Einleitung und allgemeine Informationen	4
1.1 Der Offene Katalog kommunaler Softwareanforderungen	4
1.2 Hinweise zur Darstellung der Programmanforderungen	5
1.3 Prüfleistungen zum Anforderungskatalog	8
2. Der fachübergreifende Anforderungskatalog	9
2.1 Inhaltlicher Fokus	9
2.2 Verweise auf Gesetze, Vorschriften und Normen	9
2.3 Fachgremium zum Anforderungskatalog (OKKSA Center FÜ.B)	11
3. Programmanforderungen	12
FÜ01 Informationsdarstellung	12
FÜ02 Programminteraktion	16
FÜ03 Berechnungen im Programm	22
FÜ04 Allgemeiner Zugriffsschutz	22
FÜ05 Personendatensperrung, –auskunft, und –übermittlung	30
FÜ06 Schutz von Stamm- und Bewegungsdaten	30
FÜ07 Zuverlässigkeit und Service	33
FÜ08 Programmdokumentation	35
FÜ09 Schnittstellen	42
FÜ10 Mandantenfähigkeit	44
FÜ11 Internetgestützte Programmnutzung	44
FÜ12 Komponenten zur Unterstützung der elektronischen Signatur	47

Änderungsübersicht

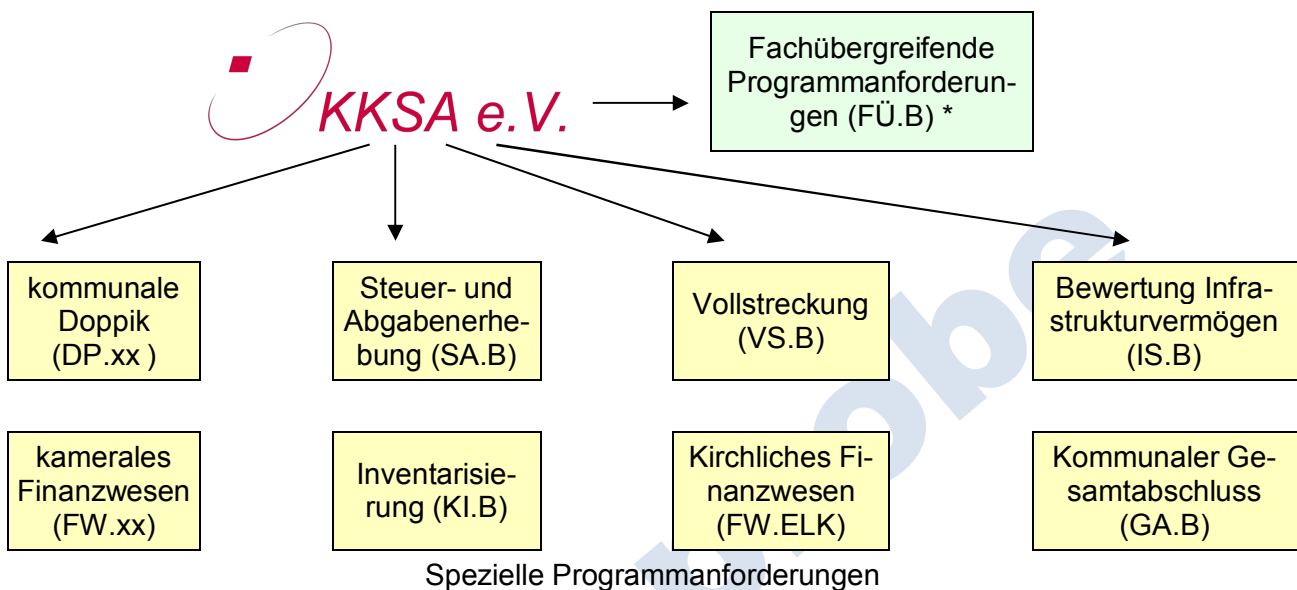
Ausgabe	Hinweise
4→5	<ul style="list-style-type: none"> • Gesetzesgrundlagen aktualisiert • Fachgremiumsänderungen • GoBD neu eingearbeitet • Vertiefung Dokumentation Zugriffsrechte • Geltungsbereich Mobile Datenverarbeitung (MDV) eingeführt • Datenart HSV (Hauptsachverhalt) ergänzt • Umfang Dokumentation definiert • Vertiefung Anforderungen an Änderungsdocumentation • Ort der Datenverarbeitung spielt eine Rolle • Prüfhinweise ergänzt • zahlreiche Kriterien korrigiert (s. Korrekturvermerke bei den Kriterien) • allgemeine Fehlerkorrektur

1. Einleitung und allgemeine Informationen

1.1 Der Offene Katalog kommunaler Softwareanforderungen

Der Offene Katalog kommunaler Softwareanforderungen (OKKSA e. V.) ist eine Initiative für die Harmonisierung von Qualitätskriterien für Software im Verwaltungseinsatz. Im Rahmen einer Internetplattform (www.okksa.de) werden gemeinsame Anforderungen der Verwaltungen an Fachprogramme für die einzelnen Aufgabenbereiche diskutiert und verabschiedet.

Resultat dieser Diskussions- und Abstimmungsprozesse sind Software-Anforderungskataloge einerseits zu speziellen Aufgabenbereichen der Verwaltungen (z. B. Erhebung von Abgaben) und andererseits ein fachübergreifender Anforderungskatalog, welcher aufgabenübergreifende Aspekte der Softwarequalität beschreibt, s. nachfolgende Skizze:



*Kürzelverwendung:

Zur einheitlichen Kennzeichnung der einzelnen Anforderungsbereiche werden Kürzel verwendet. Die Buchstaben vor dem Punkt kennzeichnen das Fachgebiet, die Buchstaben danach den regionalen Geltungsbereich eines Kataloges (B = bundesweit, ansonsten Bundeslandkürzel).

Die Anforderungskataloge ermöglichen Programm Benutzern, –entwicklern und Prüfstellen die einheitliche Feststellung der Eignung von Programmen für bestimmte Einsatzbereiche der Verwaltung. So wird nachhaltig eine Qualitätsverbesserung unterstützt.

Ziel ist die Beschreibung eines Qualitätsniveaus, welches mindestens vorhanden sein muss, um ein rechts- und normenkonformes Arbeiten der betroffenen Programm Benutzern seitens der Software sicher zu stellen. Anders ausgedrückt: ein Programm, welches alle Programmanforderungen der zutreffenden OKKSA-Kataloge erfüllt, kann eigentlich nicht mehr die Ursache für eine gesetzes- oder normenwidrige Vorgangsbearbeitung sein.¹

Die Anforderungen basieren auf gesetzlichen Vorgaben und lehnen sich an etablierte Prüfgrundlagen und Normen², die in Wirtschaft und Verwaltung Anwendung finden, an und ermöglichen die Nachnutzung vorhandener Qualitätsnachweise sowie die Unterstützung weitergehender Anforderungen.

Die Kataloge sind (im Maße ihrer Fertigstellung) frei verfügbar (es fallen Aufwandspauschalen des OKKSA e. V. an) und können u. a. für folgende Zwecke verwendet werden:

- Checklisten für Ausschreibungen,

¹ Es ist zu beachten, dass auch die beste Software bei nicht kompetenter Anwendung zu Bearbeitungsfehlern führen kann. Die Betrachtung der Aspekte des korrekten Programmeinsatzes vor Ort ist Thema weitergehender Checklisten sowie entsprechender Lehrgänge.

² Aus Normen werden im Unterschied zu Grundsätzen in der Regel geringer gewertete Anforderungen abgeleitet (KANN-Kriterien). Im Kontext zu Gesetzen und Verordnungen können Normen allerdings auch zur verbindlichen Grundlage für Programmfunktionen werden und erhalten eine höhere Wichtung.

- Pflichtenhefterstellung,
- Zertifizierung und Prüfung,
- entwicklerinterne Abnahmen.

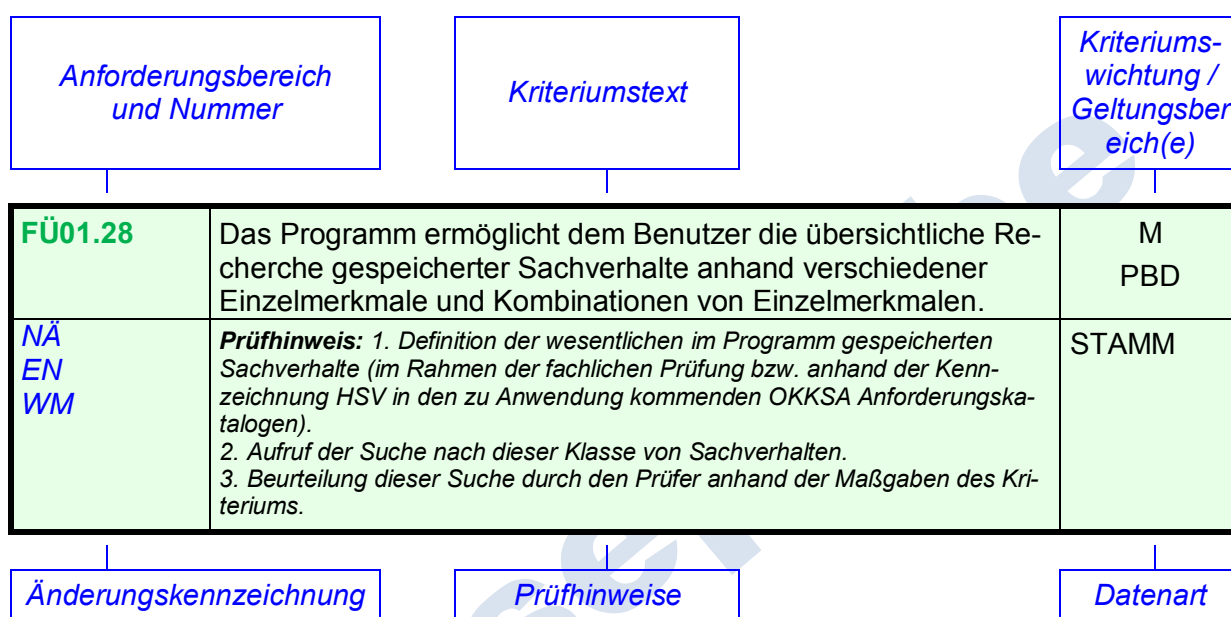
Es ist zu beachten, dass die OKKSA-Kataloge nicht den Anspruch erheben, Prüfanweisungen zu sein. Für eine neutrale Prüfung auf Basis der Kataloge sind zusätzlich Testunterlagen, Prüfanweisungen und abgestimmte Verfahren notwendig. Diese liegen in der Hoheit der jeweiligen prüfenden Einrichtungen.

Die Arbeitsweisen des Offenen Katalogs kommunaler Softwareanforderungen, die aktuell existierenden Fachgremien (OKKSA-Center) und Fachkataloge, die beteiligten Spezialisten und Partner sowie viele andere Informationen können direkt im Internet unter

www.okksa.de

abgerufen werden.

1.2 Hinweise zur Darstellung der Programmanforderungen



Anforderungsbereich und Nummer

Die Anforderungen sind in Form von einzelnen Kriterien als Sollfunktionen von Programmen formuliert. Die Kriterien sind übergreifend durch eindeutige Kürzel gekennzeichnet, welche den Anforderungsbereich kennzeichnen (hier z. B. **FÜ**, also fachübergreifende Anforderungen), gefolgt von der Nummer des Kriteriumsgebietes (hier **01**) und der Nummer des einzelnen Kriteriums innerhalb des Bereichs (hier **03**).

Kriteriumstext

Textliche Formulierung einer einzelnen Programmanforderung. Die Formulierung als Kriterium soll eine eindeutige ja/nein - Erfüllungssituation ermöglichen. Mögliche Interpretationsspielräume sind in der Erläuterung zum Kriterium zu betrachten.

Kriteriumswichtung

Es wird unterschieden zwischen **KANN**- und **MUSS**-Kriterien. Damit ist es beim Nachweis der Programmqualität möglich, Parameter zu erfassen, die eine über den Mindeststandard hinausgehende Qualitätsaussage ermöglichen. Auch können künftige **MUSS**-Anforderungen vorab als **KANN**-Anforderungen aufgenommen werden.

Die Kriteriumswichtung wird farblich gekennzeichnet:

hellgrüner Hintergrund
MUSK-Kriterium

hellgelber Hintergrund
KANN-Kriterium

Geltungsbereiche

Hier erfolgt eine Kennzeichnung eines oder mehrerer Geltungsbereiche eingeschränkt gültiger Kriterien. Geltungsbereiche können z.B. Bundesländer sein (vor allem im kommunalen Finanzbereich) oder bestimmte Funktionsbereiche der Software, die Bedingung für die Wirksamkeit des Kriteriums sind.

Im Kriterienkatalog FÜ.B werden folgende Geltungsbereiche verwendet:

PBD PersonenBezogene Daten

Im Programm treten personenbezogene Daten als Primärdaten auf (also nicht nur in Logdateien oder Daten der Programmbenutzer).

MDV Mobile DatenVerarbeitung

Das Programm verfügt über Ansichts- und Verarbeitungskomponenten, die Programmdateien auf einem mobilen Gerät (z. B. Smartphone) speichern bzw. verarbeiten. Die mobile Nutzung des Programms unter Zugriff auf gespeicherte personenbezogene Daten ist dabei explizit als Nutzungsszenario konzipiert.

***Beispiel:** Ein Programm zur Erhebung der Straßenreinigungsgebühr unterstützt die mobile Erfassung von Straßenverhältnissen mit Hilfe einer mobilen Smartphone-Lösung. Damit werden zu einzelnen Grundstücksobjekten (und damit indirekt Personen) gebührenrelevante Sachverhalte erfasst.*

In diesem Fall sind die dafür genutzten mobilen Programmkomponenten nach den MDV-Kriterien zu prüfen.

IOB InternetOrientierte Bedienung

Das Programm kann über das Internet (nicht ausschließlich Intranet) mit Standard-Browsern als Bedienoberfläche genutzt werden (betr. Kapitel **FÜ11**). Das entspricht im Wesentlichen dem Szenario einer Cloud-Lösung.

***Beispiel:** Ein Finanzprogramm kann ohne weitere Vorort-Installation allein mit dem Browser (und eventuellen Add-ons) für die Bearbeitung von Finanzvorgängen genutzt werden. In diesem Fall sind die IOB-Kriterien mit zu nutzen.*

SIG SIGNaturverwendung

Im Programm werden qualifizierte Signaturkomponenten verwendet (betr. Kapitel **FÜ12**).

Die Geltungsbereiche im Kriterienkatalog FÜ.B sind keine Optionen, die im Rahmen eines Prüfverfahrens frei gewählt werden können. Vielmehr entscheiden die tatsächlichen Programmmerkmale darüber, ob die entsprechenden Kriterien mit geprüft werden müssen.

Das jeweilige FÜ-Kriterium wird nur dann prüfrelevant, wenn die mit den angegebenen Geltungsbereichen definierten Bedingungen gegeben sind.³

***Prüfhinweis:** Der Prüfbericht soll eine Erklärung erhalten, welches der Merkmale des Programms zutrifft.*

Änderungskennzeichnung

Allgemeine Kennzeichnung der Änderungen im Kriterium gegenüber der letzten Ausgabe des Kriterienkataloges.⁴

Die Kennzeichnung erfolgt mit zwei Buchstaben, wobei der erste bezeichnet, was geändert wurde, der zweite wie geändert wurde:

³ Ein Kriterium mit der Kennzeichnung

M

MDV

PBD

ist also ein MUSS-Kriterium, welches allerdings nur dann prüfrelevant ist, wenn unter den hier genannten Bedingungen sowohl MDV als auch PBD zutreffen.

⁴ Änderungen im Rahmen einer Abstimmungsrunde eines Fachgremiums sind zunächst durch Änderungsmarkierungen und Kommentare dazu gekennzeichnet, die hier beschriebene Änderungskennzeichnung erfolgt erst bei den freigegebenen Katalogen.

Erster Buchstabe (Was wurde geändert?)	Zweiter Buchstabe (Wie wurde geändert?)
<i>K</i> – Ganzes Kriterium	<i>N</i> – Neu
<i>R</i> – Rechtsverweis	<i>Ä</i> – GeÄndert
<i>N</i> – KriteriumsNummer	<i>L</i> – GeLöscht
<i>T</i> – KriteriumsText	<i>E</i> – Erweitert
<i>G</i> – Geltungsbereich	<i>F</i> – UmFormuliert
<i>E</i> – Erläuterung	<i>R</i> – Reduziert
<i>W</i> – KriteriumsWichtung	<i>M/K</i> – Wichtung auf MUSS/KANN
<i>D</i> – Datenart	<i>S/B</i> – Datenart auf STAMM/BEW
<i>P</i> – Prüfhinweis	

Die im obigen Beispiel angeführte Kennzeichnung *NÄ, EN, WM* bedeutet also, dass das Kriterium im Vergleich zur letzten verabschiedeten Version des Kriterienkataloges (1) eine andere Nummer hat, (2) eine Erläuterung hinzugefügt wurde und (3) die Wichtung von KANN auf MUSS gesetzt wurde.

Hinweis: Änderungskennzeichnungen werden selbst nicht als Änderung gekennzeichnet.

Prüfhinweise

Mit Ausgabe 5 dieses Kriterienkataloges werden Prüfhinweise eingeführt. Sie sollen helfen, eine einheitliche Prüfung der aufgeführten Kriterien sicherzustellen. Damit bilden sie eine Maßgabe für Prüfer und gleichzeitig ein Kontrollelement der Zertifizierung (Abnahme der Prüfung) durch Aufsichtsstellen.

Datenart

In bestimmten Fällen repräsentieren die Kriterien konkrete im Programm zu speichernde Sachverhalte bzw. Informationen. Diese Daten können übergreifend für alle Anforderungskataloge Kategorien (Datenarten) zugeordnet werden, die an dieser Stelle vermerkt werden.

Gegenwärtig verwendete Datenarten:

STAMM

Stammdaten sind zustandsorientiert und dienen der Identifizierung, Klassifizierung und Charakterisierung von Sachverhalten.

Beispiel: *Personenkonto, Hinterlegung einer Berechnungsformel*

BEW

Bewegungsdaten sind ablauforientiert und entstehen immer wieder neu durch betriebliche Leistungsprozesse. Sie bewirken die Veränderung von Bestandsdaten. Bewegungsdaten widerspiegeln einmalige Ereignisse, die keiner nachträglichen Veränderung unterliegen. Das bedeutet z.B., dass ein Anordnungsdatensatz, der noch in ändernder Bearbeitung ist, in diesem Stadium noch kein Bewegungsdatum ist. Erst eine Buchung macht aus den vorerfassten Informationen zu schützende Bewegungsdaten.

Beispiel: *Buchung, Druckdatei*

Für die Speicherung so gekennzeichnete Stamm- und Bewegungsdaten gelten funktionale Programmanforderungen (z.B. Protokollierung von Änderungen, Zeitstempel), die im fachübergreifenden Anforderungskatalog (Kapitel "Schutz von Stamm- und Bewegungsdaten") beschrieben sind.

Weitere Kennzeichnungen bei "Datenart":

HSV

Hauptsachverhalt

Mit dem so gekennzeichneten Kriterium werden Hauptsachverhalte eines fachlichen Softwareanwendungsgebietes charakterisiert. Für deren Darstellung und Recherche gelten besondere Anforderungen.

Beispiel: *"Objekt" bei der Grundstücksveranlagung, "Debitor" bei der Buchführung.*

1.3 Prüfleistungen zum Anforderungskatalog

Mit dem vorliegenden Anforderungskatalog entsteht die Möglichkeit, im Auftrag von Anwendern und Anbietern entsprechender Softwarelösungen Konformitätsnachweise zu erstellen. Innerhalb der OKKSA-Plattform werden entsprechende Prüfmöglichkeiten mit Kooperationspartnern bereitgestellt.

Die TÜV Informationstechnik GmbH (TÜViT) fördert die OKKSA-Idee durch Bereitstellung eines Umfeldes für die Durchführung von fachlichen Prüfungen nach den im OKKSA-Center FÜ.B abgestimmten und im Katalog aufgeführten Kriterien. Dazu wird durch die TÜViT-Zertifizierungsstelle das Prüfzeichen „Geprüftes Fachprogramm“ bereitgestellt, bei dem immer auch ein weiterer fachspezifischer Kriterienkatalog zur Anwendung kommt.



© TÜViT – TÜV NORD GROUP – www.tuvit.de

Die Prüfungen zu diesem Zeichen werden durch bei TÜViT akkreditierte Prüfer durchgeführt. Eine aktuelle Liste dazu ist unter

<http://www.tuvit.de/gfp>

zu finden. Informationen zum Status von Prüfungen nach diesem Kriterienkatalog sind unter www.okksa.de/status zu finden.

Leseprobe

2. Der fachübergreifende Anforderungskatalog

2.1 Inhaltlicher Fokus

Die fachübergreifenden Programmanforderungen (FÜ.B - Kriterien) beschreiben Aspekte der Softwarequalität, welche gleichermaßen für Programme verschiedener Einsatzbereiche zutreffend sind. Dieser Anforderungsbereich wurde eingerichtet, um zu vermeiden, dass gleichartige Programmanforderungen redundant in verschiedenen Katalogen diskutiert werden. Gleichzeitig werden grundsätzliche (generische) Anforderungen formuliert, welche ihrerseits Richtlinie für die Formulierung weitergehender fachspezifischer Programmanforderungen sind.

Bei der Feststellung der Qualität eines Programmproduktes nach OKKSA ist der fachübergreifende Anforderungskatalog grundsätzlich immer mit zu verwenden. Allerdings sind die formulierten Anforderungen anhand spezifischer Testdaten für den jeweiligen Anwendungsbereich zu validieren.⁵

2.2 Verweise auf Gesetze, Vorschriften und Normen

Über den einzelnen Kriterien erfolgt ggf. ein Verweis auf Gesetze und Normen, die die Forderung des Kriteriums begründen, konkretisieren oder vergleichbar machen. Dabei wird neben bundeslandübergreifenden Regelungen auch auf landesspezifische Gesetze verwiesen. Die Verweise sind an dieser Stelle beispielhaft und nicht abschließend.

Im Einzelnen besteht bei den einzelnen Kriterienbereichen ein Bezug zu folgenden Unterlagen:

auf Bundesebene

[AO]	Abgabenordnung, Stand 20.11.2015
[BDSG]	Bundesdatenschutzgesetz, Stand 25.02.2015 (verwiesen wird insbesondere auch auf die Anlage zu § 9)
[BDSG_A9]	Bundesdatenschutzgesetz (BDSG) Anlage (zu § 9 Satz 1)
[DSG_EKD]	Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland Stand 1.2.2013
[HGB]	Handelsgesetzbuch, Stand 20.11.2015
[SigG]	Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG), Stand 07.08.2013
[VwVfG]	Verwaltungsverfahrensgesetz, Stand 20.11.2015

auf Landesebene

[KVO]	Gemeindekassenverordnungen der Bundesländer, hier beispielhaft: [KVO] HE Hessische Verordnung über die Kassenführung der Gemeinden (Gemeindekassenverordnung – GemKVO) vom 27. Dezember 2011 (GVBl. I S. 830, GVBl. 2012 S. 19)
[HVO]	Gemeindehaushaltsverordnungen der Bundesländer, hier beispielhaft: [HVO] NW Verordnung über das Haushaltswesen der Gemeinden im Land Nordrhein-Westfalen, Stand 18.07.2013
[DSG]	Datenschutzgesetze der Bundesländer, hier beispielhaft: [DSG] SN Sächsisches Datenschutzgesetz 2003, Stand 29.04.2015 [DSG] SH Landesdatenschutzgesetz Schleswig-Holstein 2000, Stand 16.03.2015

⁵ **Beispiel:** Das Kriterium FÜ2.5 fordert, dass bei der Eingabe von Werten bei Erfassungsmasken die formale Plausibilität dieser Werte durch das Programm überwacht wird. Um den Nachweis zu führen, dass z.B. ein Programm zur elektronischen Vergabe von Leistungen (Katalog OV.B) diese Anforderung erfüllt, ist als Testfall z.B. das Ausfüllen eines Bekanntmachungsformulars geeignet.

Grundsätze

- [GoB] Grundsätze ordnungsmäßiger Buchführung.
- [GoBS] Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme, BStBl 1995 I S. 738⁶
- [GoBD] Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff
Schreiben des BMF vom 14.11.2014⁷

Normen und Standards (im Katalog konkret verwiesen)

- [ISO25051] ISO/IEC 25051:2014-02 Software-Engineering – System- und Software-Qualitätsanforderungen und Evaluation (SQuaRE) - Qualitätsanforderungen an Ready to Use Software Products (RUSP) und Prüfverfahren
- [ISO9241] EN ISO 9241 Ergonomie der Mensch-System-Interaktion, Stand 2006
Verweise auf:
[ISO9241]-303 Anforderungen an elektronische und optische Anzeigen
[ISO9241]-11 Anforderungen an die Gebrauchstauglichkeit - Leitsätze
[ISO9241]-13 Benutzerführung
[ISO9241]-110 Grundsätze der Dialoggestaltung
- [PS880] Prüfstandard des Instituts der Wirtschaftsprüfer: Die Prüfung von Softwareprodukten (Stand 11.03.2010)
- [IDW_FAIT1] IDW RS FAIT 1 "Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie", "Die Wirtschaftsprüfung" 21/2002, S. 1157 ff., FN-IDW 11/2002, S. 649 ff.
- [IDW_FAIT5] IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Dienstleistungen einschließlich Cloud Computing vom 04.11.2015
- [EVBIT_SYS] EVB-IT Systemvertrag V2.01, Stand 09.01.2013 (Teil der "Ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen"⁸)

Weitere Prüfnormen

- Verwaltungsvorschrift der Sächsischen Anstalt für kommunale Datenverarbeitung: Prüfhandbuch über die erforderlichen technischen Standards für Programmzulassungen im Bereich der Allgemeinen Anforderungen an Finanzverfahren nach den Regeln der Doppik (VwV Prüfhandbuch AP.Doppik – VwV PHB-AP.Doppik)⁹
- Anforderungskatalog v 2.0 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH vom 28.11.2014 (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)¹⁰
- IT-Grundsatz-Kataloge - Standard-Sicherheitsmaßnahmen, BSI, jährlich neu, Stand 2014¹¹
- BSI IT-Grundsatz-Standards, Stand 2008¹²

⁶ Die GoBS wurden trotz der neuen GoBD vorerst als Verweis beibehalten, da sie noch in Haushaltsverordnungen verwiesen werden. Künftig soll dieser Verweis entfallen.

⁷ Die Anwendbarkeit der GoBS und GoBD in den einzelnen Bundesländern ist unterschiedlich, weshalb beide verwiesen werden. Zu beachten ist aber, dass beide genauso wie die einschlägigen Regelungen der Haushaltsverordnungen zunächst die Organisation des DV-Einsatzes im Finanzwesen im Blickpunkt haben, hinsichtlich der Anforderungen an die Programme sind sie also eine indirekte Vorgabe.

⁸ siehe: de.wikipedia.org/wiki/EVB-IT

⁹ siehe www.revosax.sachsen.de/vorschrift/14190-VwV_Pruefhandbuch_AP_Doppik

¹⁰ siehe www.datenschutzzentrum.de/uploads/quetesiegel/quetesiegel-anforderungskatalog.pdf

¹¹ https://www.bsi.bund.de/DE/Themen/ITGrundsatz/ITGrundsatzKataloge/itgrundschutzkataloge_node.html

¹² https://www.bsi.bund.de/DE/Themen/ITGrundsatz/ITGrundsatzStandards/ITGrundsatzStandards_node.html

2.3 Fachgremium zum Anforderungskatalog (OKKSA Center FÜ.B)

Dem fachlichen Abstimmungsgremium zu diesem Anforderungskatalog (OKKSA-Center FÜ.B) gehören folgende Personen an:

1. Dr. Uwe Schwochert, TRUSTBIT - Redaktion,
2. Georg Bollmann, Stadt Dortmund,
3. Stephan Di Nunzio, Zertifizierungsstelle bei TÜV Informationstechnik GmbH,
4. Carsten Gerlach, TCI Rechtsanwälte Berlin,
5. Dr. Axel Gutenkunst, Evangelische Landeskirche Württemberg,
6. Oliver Maas, Kommunales Forum für Informationstechnik Schleswig Holstein,
7. Ludwig Maiworm, Hochtaunuskreis,
8. Marcus Meiners, Gemeindeprüfungsanstalt NRW,
9. Lars Riedel (Datev e. G.) als Vertreter des Herstellerbeirates,
10. Christian Prietz, Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein,
11. Dr. Karen Verbist, Stadt Marburg,
12. Roland Wolf, Softwarequalität und Prüfung in der öffentlichen Verwaltung.

Die Vorgehensweise der fachlichen Abstimmung der nachfolgenden Kriterien folgt den Vorgaben des OKKSA e. V., festgehalten in der "Geschäftsordnung OKKSA-Center". Informationen zur Tätigkeit des OKKSA e. V. sowie die Texte der Geschäftsordnungen sind unter www.okksa.de/vereinsinfo zu finden.

Leseprobe

3. Programmanforderungen

FÜ01 Informationsdarstellung

Die nachfolgenden Kriterien betreffen u. a. auch wichtige Aspekte der Bedienbarkeit (Usability) des Programms. Im Unterschied zu den etablierten Usability-Normen aus [ISO9241] (z. B. [ISO9241]-110 / [ISO9241]-11), welche zur Konformitätsbeurteilung eine Einzelfallbeurteilung der Anwendungssituation¹³ erforderlich machen, steht hier jedoch eine einzelfallübergreifende Beurteilung der Bedienbarkeit des Programms im Vordergrund. Vor dem Hintergrund der GoB sowie deren Umsetzungen in Gesetzen soll das Programm also zunächst eine sichere und prüfbare Speicherung von Sachverhalten und Steuerung von Programmfunktionen ermöglichen.

Anders ausgedrückt: Das Programm soll in seiner Gestaltung nicht selbst potentielle Quelle von Fehlbedienungen oder Fehleinschätzungen zu den gespeicherten Informationen sein. Aspekte wie die Bedieneffizienz und der Bedienkomfort sind dagegen nur nachrangig von Bedeutung.

Sollte die Usability des Programms im Vordergrund der Betrachtung stehen, so wird die Anwendung entsprechender etablierter Prüfverfahren auf Basis der [ISO9241] empfohlen.

Vgl. [KVO] HE § 5 Abs. 5 Nr. 2; [HVO] NW § 27 Abs. 2, 5; [HGB] § 238 Abs. 1, § 239 Abs. 2, [GoBD] Nr. 30, 32, 44

FÜ01.01	Im Programm können Sachverhalte nachvollziehbar und wirklichkeitsgetreu eingegeben und gespeichert werden. Wenn ein Programm einen bestimmten Sachverhalt verarbeiten kann, muss dieser für einen sachverständigen Dritten erkennbar sein.	M
RÄ PN	Prüfhinweis: <i>1. Definition der wesentlichen im Programm gespeicherten Sachverhalte (im Rahmen der fachlichen Prüfung bzw. anhand der Kennzeichnung HSV in den zu Anwendung kommenden OKKSA Anforderungskatalogen).</i> <i>2. Aufruf einer oder mehrerer Ansichts-/ Bearbeitungsmasken bzw. einer Listenauskunft zu dieser Klasse von Sachverhalten.</i> <i>3. Beurteilung der Klarheit der Darstellung durch den Prüfer anhand der Maßgaben des Kriteriums.</i> <i>4. Überwachung der Klarheit auch bei anderen Sachverhalten (die nicht als HSV gekennzeichnet sind).</i>	

Die Umsetzung dieser Anforderung ist eine wesentliche Grundlage für eine transparente und vor Ort prüfbare Programmnutzung. Sie gilt für alle im Programm gespeicherten Fachdaten. Die Erfüllung dieser Anforderung ist im engen Kontext zum jeweiligen Anwendungsgebiet zu sehen. Deshalb ist diese Anforderung, die an dieser Stelle zunächst einen Grundsatz widerspiegelt, in fachgebietsspezifischen Anforderungskatalogen weiter untersetzt.

Zu beachten ist, dass es hier zunächst um die programmseitigen Möglichkeiten zur Speicherung von Sachverhalten geht.

Beispiel: Ein Programm zur Abrechnung von Spesen muss verschiedene Bewirtungssachverhalte als Grundlage für die Ermittlung des täglichen Spesensatzes berücksichtigen. Diese Sachverhalte müssen auch für den ungeübten Nutzer jederzeit eindeutig erkennbar sein (z.B. „Mittagessen erhalten“, „Frühstück erhalten“). Eine Kennzeichnung in Form von „1,5 Frühstück“ erhalten (statt „1 Mittagessen erhalten“) wäre, auch wenn sie zu richtigen Spesen führt, falsch im Sinne des Kriteriums.

¹³ Gemeint sind einzelne Anwendungssituationen, die sich auf konkrete Arbeitsaufgaben des Benutzers und entsprechende Bedienungsvorgänge im Programm beziehen.

FÜ01.02	Das Programm ermöglicht dem Benutzer die übersichtliche Recherche gespeicherter Sachverhalte anhand ihrer kennzeichnenden Merkmale .	M
PN	Prüfhinweis: 1. Definition der wesentlichen im Programm gespeicherten Sachverhalte (im Rahmen der fachlichen Prüfung bzw. anhand der Kennzeichnung HSV in den zu Anwendung kommenden OKKSA Anforderungskatalogen). 2. Aufruf und Dokumentation der Suchfunktion nach diesen Sachverhalten. 3. Beurteilung der Suche durch den Prüfer anhand der Maßgaben des Kriteriums.	

Die vom Benutzer hinterlegten Daten müssen wiederauffindbar sein. Dabei genügt es nach diesem Kriterium, wenn die Daten anhand der wesentlichen Merkmale ermittelt werden können. So sollten z.B. Personendaten anhand der Anfangsbuchstaben des Familiennamens, Flurstücksdaten anhand der Gemarkungsbezeichnung gesucht werden können.

FÜ01.03	Das Programm ermöglicht dem Benutzer die übersichtliche Recherche gespeicherter Sachverhalte anhand verschiedener Einzelmerkmale und Kombinationen von Einzelmerkmalen. Dabei kann auch nach Teilzeichenketten gesucht werden.	K
TF ER PN	Prüfhinweis: 1. Definition der wesentlichen im Programm gespeicherten Sachverhalte (im Rahmen der fachlichen Prüfung bzw. anhand der Kennzeichnung HSV in den zu Anwendung kommenden OKKSA Anforderungskatalogen). 2. Aufruf und Dokumentation der Suchfunktion nach diesen Sachverhalten. 3. Beurteilung der Suche durch den Prüfer anhand der Maßgaben des Kriteriums.	

Die weitergehende Forderung dieses Kriteriums erhebt nicht Anspruch, dass die Möglichkeit zur Recherche in allen Datenfeldern bestehen muss, sondern widerspiegelt eine Grundforderung nach Recherchefunktionen.

FÜ01.04	Das Programm stellt bei der lesbaren Ausgabe die Sachverhalte für den Bearbeiter bzw. den Adressaten übersichtlich und klar dar. Die vom Programm erzeugten Dokumente sind mindestens gekennzeichnet durch: 1. les- und druckbare Schriftzeichen in hinreichender Schriftgröße, 2. sparsame und empfängerorientierte Verwendung von Abkürzungen und Fachbegriffen, 3. logische Darstellung von Zusammenhängen und Werten, 4. räumliche Anordnung von Texten und Werten, 5. zutreffende Bezeichnung des Dokumentes und seiner einzelnen Seiten, 6. Dokument-Datum, 7. Nummerierung von Seiten.	M
RE PN	Prüfhinweis: Bei allen während einer Prüfung erzeugten Dokumenten und Bildschirmabzügen ist dieses Kriterium durch den Prüfer zu überwachen.	

"Lesbare Ausgabe" meint die folgenden Arten der Informationsdarstellung:

- a) Druck eines Dokumentes auf Papier,
- b) Erzeugung eines elektronischen Abbildes eines Druckdokumentes (pdf-Druck, Seitenvorschau, ...),
- c) Darstellung von Informationen am Bildschirm.

Es ist zu beachten, dass im Fall c) die Aspekte des Seitenüberganges (Seitennummern, Seitentitel, ...) keine Rolle spielen. Spezielle Aspekte der Gestaltung längerer Bildschirmausgaben (Scrollbalken, ...) sind in diesem Kriterienkatalog nicht betrachtet.

Unabhängig von Forderungen zum gesetzlich vorgegebenen Inhalt von externen Dokumenten (z. B. bei einem Steuerbescheid) steht hier die formale Aufbereitung der Informationen im Vordergrund.

Zu 1.: "Hinreichende Schriftgröße" bezieht sich auf den Hauptinhalt eines Dokumentes / Bildschirmes. Sie kann nicht absolut festgelegt werden. So kann ein Schriftzeichen von 2mm Höhe als Fußnote durchaus akzeptabel sein, als Hauptschriftart in langen Tabellenzeilen dürfte die Lesbarkeit bezüglich wichtiger Dokumentinhalte nicht akzeptabel sein. Weitere Informationen zu diesem Thema sind u. a. in [ISO9241]-03 (Anforderungen an visuelle Anzeigen) zu finden.

Zu 2.: "Empfängerorientierte Verwendung von Begriffen" meint nicht, dass softwarespezifische Abkürzungen und Begriffe akzeptabel sind, nur weil der Programmbenutzer von ihnen in einer Schulung gehört haben müsste. Die Wahl der Begriffe und Abkürzungen soll den Gepflogenheiten des Softwareanwendungsgebietes folgen.

Zu 3.: Insbesondere bei Dokumenten mit einer gelegentlichen Zielgruppe (z. B. Bescheide für Bürger oder Übersichten für das Management) sollen komplexe Zusammenhänge zwischen den Dokumentinhalten nachvollziehbar sein.

Zu 4.: Die Anordnung der Inhalte in dem Dokument soll eine zweifelsfreie Zuordnung von Texten, Werten, Überschriften usw. ermöglichen. Das gedruckte Dokument soll Ränder haben und alle Informationen sollen lesbar sein (keine hinter den Seitenrand oder den Tabellenrand verschwindenden Informationen).

Ein Erfüllungsnachweis zu den genannten Anforderungen soll anhand eines tatsächlich vorliegenden Programms (z. B. musterhaft angepasst) und nicht anhand theoretisch möglicher Anpassungen erbracht werden.

Beispiel: Wenn ein Abgabenbescheid mehrere Seiten umfasst, so sind die Seiten zu nummerieren. Auf jeder Seite ist eine Kennzeichnung erforderlich, die eine eindeutige Zuordnung zu einem gemeinsamen Bescheiddokument ersichtlich macht. Die Gesamtseitenzahl ist kenntlich zu machen. Der Bürger (= gelegentliche Zielgruppe) soll bei durchschnittlichem Sachverstand erkennen können, wofür der Bescheid ist (Abgabearart, Tarife) und wie der Betrag hergeleitet wurde. Die wesentlichen Bescheidinhalte sollten mit einer Schrifthöhe nicht unter 2,5mm gedruckt sein. Sofern es sich um eine Fachanwendung handelt, deren normales Aufgabengebiet die Erstellung von Abgabenbescheiden ist, genügt es nicht, wenn der Anwender durch Anwendung eines Listengenerators oder ähnlicher Tools die technische Möglichkeit hat, seine Bescheide entsprechend anzupassen. Vielmehr soll der Programmentwickler entsprechende Templates für den Bescheiddruck mit ausliefern.

Vgl. [KVO] HE § 5 Abs. 5 Nr. 1; [HVO] NW § 27 Abs. 2, 5; [HGB] § 239 Abs. 4

FÜ01.04a	Die vom Programm erzeugten Dokumente enthalten Informationen zur verwendeten Programmversion.	K
RÄ		

Mit der Angabe der Programmversion kann der Prüfstatus der verwendeten Programme nachgewiesen werden. Weiterhin wird die Fehlersuche erleichtert.

FÜ01.04b	Die Bedienoberfläche der fachlichen Teile des Programms ist in deutscher Sprache ausgeführt. Dies gilt auch für die in der täglichen Benutzung notwendigen technischen Teile der Bedienoberfläche. Sonstige Elemente der Bedienoberfläche sind mindestens in englischer Sprache auszuführen.	M
KN	Prüfhinweis: Überwachung bei allen für die Prüfung relevanten Bildschirmmasken.	

Insbesondere sollen gesetzessdefinierte Fachbegriffe richtig benannt sein. "Technische Teile der Bedienoberfläche" meint z. B. nutzerorientierte Module zur Erzeugung von Druckausgaben (Report-Generator, pdf-Ausgabe) oder Module zur Berechtigungsverwaltung.

Beispiel: Der Begriff "Konto" darf nicht durch den Begriff "Account" ersetzt sein.

FÜ01.05	Alle im Programm gespeicherten Fachdaten können übersichtlich ausgedruckt werden.	M
RE EE PN	<i>Prüfhinweis: Bei der Prüfung ist zunächst eine allgemeine Druckfunktion für Bildschirmdarstellungen zu hinterfragen, die über einen systemdefinierten Bildschirmabzug hinausgeht (also übersichtliche Darstellung im Sinne von FÜ01.04) und stichprobenhaft zu dokumentieren. Gibt es diese allgemeine Druckfunktion nicht, sind die einzelnen Programmsachverhalte testweise als Ausdruck bereitzustellen. Dabei ist durch den Prüfer zu überwachen, dass zumindest die HSV übersichtlich im Sinne von FÜ01.04 ausgedruckt werden können.</i>	

Mit dieser Anforderung wird der Anspruch eines Programmanwenders auf eine unabhängige (vom technischen System) Kopie der bearbeiteten Fachvorgänge bekräftigt.

Wichtige Aspekte der übersichtlichen Darstellungen von Fachdaten sind in FÜ01.04 dargestellt.

Der Ausdruck eines Bildschirmauszuges kann an dieser Stelle in Ausnahmefällen akzeptiert werden, wenn diese Form des Ausdrucks vom Programmentwickler vorgesehen ist und die entstehenden Ausdrücke den Übersichtlichkeitsanforderungen nach Kriterium FÜ01.04 genügen. Dies gilt nicht für verbindlich vorgeschriebene Berichte, Dokumente und Auswertungen, s. z. B. [GoBD] Nr. 8.

Eine weitere Ausnahme stellen Systemeinstellungen oder sonstige Hilfsdaten im Programm dar, wenn sie keine Auswirkung auf die fachliche Vorgangsbearbeitung haben.

Beim Ausdruck sind die unter FÜ04.15 genannten Zugriffsrechte zu beachten.

***Beispiel:** Zu den Fachdaten zählen auch die gespeicherten Zugriffsrechte auf Daten und Programmfunktionen (s. FÜ04.xx) sowie die gespeicherten Benutzer und ihre Zuordnung zu Benutzertypen (FÜ04.20). Im Zusammenhang mit FÜ01.04 soll das Programm in der Lage sein, dazu eine (für einen sachverständigen Dritten) verständliche Übersicht zu drucken.*

FÜ01.06	Das Programm gestattet es (z. B. durch die Möglichkeit der Integration von Archivierungsfunktionalitäten), Druckausgaben , die einer gesetzlichen Aufbewahrungsfrist unterliegen, wiederholt inhalts- und formgleich während ihrer Aufbewahrungsfrist zu reproduzieren bzw. einer entsprechenden Archivierung zuzuführen. Die Art der Bereitstellung der Dokumente durch das Programm ermöglicht deren spätere inhaltliche Recherche.	M
RE TE EE PN	<i>Prüfhinweis: Seitens des Prüfers ist in der Regel die programminterne Archivierungsfunktion (inkl. Recherche) zu dokumentieren. Alternativ, falls diese den Anforderungen nicht genügt, ist darzustellen, wie ein (ggf. externes) Archivierungssystem an die Erzeugung der relevanten Druckausgaben (z. B. Bescheide, Rechnungen) angebunden wird (z. B. durch Verweis auf entsprechende Dokumentation) und wie aus dem Programm heraus auf dort gespeicherte Sachverhalte suchend zugegriffen werden kann.</i>	

Ein inhalts- und formgleicher Ausdruck kann eigentlich nur mit einer anerkannten Archivierungstechnologie bereitgestellt werden. Diese muss, wenn nicht integriert, so doch wenigstens anbindbar sein, die Anbindung muss dokumentiert sein. Dabei soll das Programm Druckausgaben in Form durchsuchbarer Dateien bereitstellen können.

FÜ01.07	Dokumente, die das Programm erzeugt, entsprechen den gültigen Formvorschriften .	M
RL		

Diese Anforderung ist in den einzelnen Fachanforderungskatalogen weiter vertieft.