Kommunalsoftware auf dem Prüfstand[1]

(Auszug aus der Veröffentlichung im OKKSA-Newsletter Nr. 19 vom 24.11.09)

Teil 8: Wer hat meine Adressdatei? Datenschutz in Fachverfahren.
(von Dr. Uwe Schwochert)

Bei der Anwendung der fachübergreifenden Kriterien (FÜ.B) zur Prüfung und Bewertung von Fachverfahren ist der Datenschutz zunächst nur ein Teilaspekt. Es gibt Prüfverfahren (wie das Datenschutzgütesiegel), die hier deutlich detailliertere Anforderungen stellen. Doch auch bei nach OKKSA FÜ.B geprüften Verfahren soll der Anwender sicher sein können, dass wichtige Programmfunktionen, die er für die Umsetzung von Datenschutzvorgaben im Programm benötigt, vorhanden sind.

Entsprechende Kriterien finden sich verteilt auf fast allen Kapitel des fachübergreifenden Anforderungskataloges, z. B. FÜ4 (Zugangskontrolle und zur Benutzerrechteverwaltung), FÜ6 (Datenprotokollierung) und FÜ8 (Programmdokumentation).
Im heute zu besprechenden Kapitel 5 des Kriterienkataloges sind Anforderungen zusammengefasst, die ausschließlich unter Datenschutzaspekten aufgenommen wurden.

Bei der Formulierung der Anforderungen im fachübergreifenden Kriterienkatalog wurde von Folgendem ausgegangen:
1. Fast in jedem im Verwaltungsbereich eingesetzten Fachverfahren werden mehr oder weniger sensible personenbezogene Daten gespeichert.
2. Der datenschutzgerechte Umgang mit diesen Daten erfordert grundlegende Programmmechanismen, ohne die es dem Anwender nicht möglich ist, eine datenschutzgerechte Vorgangsbearbeitung zu organisieren.
3. Im Kontext der fachbezogenen Vorgangsbearbeitung definieren sich weitergehende Anforderungen an die datenschutzgerechten Speicherung, die nicht Gegenstand der fachübergreifenden Anforderungen sind.

Betrachtet werden also allgemeine Funktionen der Software, die zur Verarbeitung personenbezogener Daten benötigt werden. Das hier besprochene Kapitel 5 enthält dabei besondere Programmanforderungen aus Datenschutzsicht, die in den anderen Kapiteln nicht mit abgedeckt werden.

Eine grundsätzliche Datenanforderung, die sich aus den Grundsätzen Zweckbindung und Datensparsamkeit ergibt, ist

[FÜ05.01] Das Programm unterstützt die Löschung von personenbezogenen Daten durch den Bearbeiter.[MUSS-Kriterium]

Es muss also einen Mechanismus geben, wie gespeicherte personenbezogene Daten (z. B. Adressen aus dem Bereich der Abgabenerhebung) aus dem Datenbestand gelöscht werden können. Gründe dafür könnten z. B. fälschlicherweise gespeicherte Adressen und Sachverhalte zu Bürgern oder auch Löschfristen für Nutzungsprotokolle des Programms sein. Diese Anforderung ist nicht trivial, da die betrachteten personenbezogenen Daten durchaus komplex mit anderen gespeicherten Informationen verknüpft sein können. Deshalb muss es dann auch möglich sein, entsprechende Verknüpfungen wieder zu löschen oder wenigstens die entsprechenden Informationen zu pseudonymisieren.

[1] Hinweis: Die in der Artikelserie genannten Kriterien stammen aus der aktuellen Fassung des "OKKSA Anforderungskatalogs für Fachprogramme in der Öffentlichen Verwaltung - Teilbereich Fachübergreifende Programmanforderungen", Version 3.1

Spätestens in dem Moment, wo bereits finanzwirksame Vorgänge mit den gespeicherten Daten verknüpft sind, ist die Löschung nicht mehr ohne weiteres möglich. In diesem Fall soll aber trotzdem die Benutzung dieser Informationen technisch behindert werden können:

[FÜ05.02] Im Programm kann die Weiterverarbeitung von Daten einer Person durch Sperrkennzeichen verhindert werden. [MUSS-Kriterium]

Mit dieser Funktion soll der Bearbeiter programmseitig unterstützt werden, die als gesperrt gekennzeichneten Daten nicht versehentlich weiter zu verwenden. Dies setzt eine entsprechende Kennzeichnungsmöglichkeit im Programm voraus.

Entsprechend [BDSG] § 19 hat jeder "Betroffene", das heißt, jede Person, zu der Informationen in dem Fachverfahren gespeichert sind, ein Recht auf eine Auskunft zu den gespeicherten Informationen. Aus Sicht des Programmanwenders gibt es bei dieser Beauskunftung mehrere Probleme: Zum einen muss er, insbesondere bei einem für verschiedene Aufgabenbereiche eingesetzten Verfahren, erst einmal wissen, wo überall im Verfahren personenbezogene Informationen gespeichert sind. Dies betrifft nicht nur primäre Sachdaten, wie Steuersachverhalte oder Zahlungsinformation. Genauso sind meist auch historische Sachverhalte (Vorgänge vorheriger Perioden oder alte Werte korrigierter Felder) gespeichert, deren Vorhandensein leicht in Vergessenheit gerät. Zum anderen muss der Anwender auch wissen, dass bestimmte personenbezogene Informationen gespeichert werden, wie z. B. Logging-Protokolle der Programmanwender und scheinbar gelöschte Datensätze.

So ergibt sich, dass nicht nur der auskunftsberechtigte Betroffene sondern auch der verantwortungsbewusste Programmanwender eine Unterstützung benötigt, um einen Überblick über die gespeicherten personenbezogenen Informationen zu erhalten. Auch wenn das primär eine Anforderung an die Programmdokumentation ist, ist es doch außerordentlich hilfreich, wenn das Programm diese Auskunft auch funktional unterstützt:

[FÜ05.03] Das Programm unterstützt eine spezielle Auskunftsfunktion für die Darstellung aller zu einer Person gespeicherten Informationen. [KANN-Kriterium]

Seitens der Pogrammdokumentation (Kriterien FÜ08.xx) sind entsprechende Hinweise in jedem Fall erforderlich. Mit Kriterium FÜ08.09 wird weitergehend eine direkte Unterstützung der Erstellung des Verfahrensverzeichnisses gefordert:

[FÜ08.09] Das Programm oder die Programmdokumentation unterstützt die Beschaffung und Verwaltung folgender für die Erstellung des Verfahrensverzeichnisses notwendigen Informationen:
1. Name und Anschrift der datenverarbeitenden Stelle,
2. Name des eingesetztes Verfahren,
3. Zweckbestimmung und Rechtsgrundlage des Verfahrens,
4. Kreis der Betroffenen,
5. zugriffsberechtigte Personen. [KANN-Kriterium]

Punkt 4 impliziert auch eine konkrete Auflistung der gespeicherten personenbezogenen Datenarten, diese Anforderung soll in Version 4 des Kriterienkataloge weiter konkretisiert werden.

Dort, wo besonders sensible Sachverhalte gespeichert sind, kann es erforderlich werden, neben den in FÜ06.xx beschriebenen Protokoll- und Zeitstempelfunktionen (s. Fachbeitrag

im nächsten Newsletter) auch zu erfassen, dass personenbezogene Daten recherchiert werden:

[FÜ05.04] Beim Zugriff auf personenbezogene Daten kann protokolliert werden, welche Selektionskriterien wann und von wem benutzt worden sind. [KANN-Kriterium]

Diese Funktion spielt vor allem bei der über mehrere Bereiche oder auch Organisationen verteilten Datenverarbeitung eine Rolle (z. B. auch Fernwartung, Home-Office). Durch Protokollierung kritischer personenbezogener Datenzugriffe kann so zumindest festgestellt werden, wenn Daten in größerem Umfang recherchiert werden, die potentiell extern missbraucht werden könnten. Aktuelle Datenschutzpannen bei Social Communities und Finanzdienstleistern machen deutlich, wie wichtig entsprechende Mechanismen sind.

Bei dieser Betrachtung spezieller Programmfunktionen zur Unterstützung des Datenschutzes darf aber nicht vergessen werden, dass die programmseitige Unterstützung des Datenschutzes eine sehr weitgehende Anforderungsdimension ist. Dabei ist eine sichere und kontrollierte Programmbedienung einer der wichtigsten Faktoren. Ob diese möglich ist, hängt von sehr vielen Faktoren ab, die auch den Rahmen von OKKSA FÜ.B sprengen.

Nächster Teil der Serie: Haben Stammdaten Jahresringe? Zeitstempel und Historien im Kontext der GoB.