Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Handreichung für Datenschutzbeauftragte

Thema:

Strukturierungsvorschlag für eine datenschutzkonforme Dokumentation nach LDSG und (neuer) DSVO

Stand: 06.09.2011

Die überarbeitete Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten (Datenschutzverordnung - DSVO) vom 9. Dezember 2008 (Geltungsbeginn: 1. Januar 2009) gibt dem Datenschutzbeauftragten bzw. dem für die Dokumentation Verantwortlichen viele Gestaltungsmöglichkeiten bei der Dokumentation der automatisierten Datenverarbeitung. Die neue DSVO beschreibt in ihrem Text, was dokumentiert werden muss, legt aber nicht fest, in welcher Form.

Eine gut strukturierte, transparente und vollständige Dokumentation ist aber nicht einfach „aus dem Ärmel zu schütteln“. Vielmehr ist es schwierig, den Gesamtzusammenhang zwischen konzeptioneller Vorarbeit und laufender Systemdokumentation, organisatorischen und technischen Regelungen, Differenzierung einzelner automatisierter Verfahren und den Revisionsinstrumenten nicht zu verlieren und somit die Übersicht zu behalten. Dieses Dokument stellt einen Strukturierungsvorschlag vor, der als ein modulares Beispiel für eine ordnungsgemäße Dokumentation nach LDSG und DSVO angesehen werden kann.

Dieser Vorschlag soll auf keinen Fall eine „Vorschrift“ darstellen. Er soll den Verantwortlichen lediglich eine Empfehlung in Form eines Beispiels an die Hand geben, wie eine datenschutzkonforme Dokumentation sowohl strukturiert als auch übersichtlich erstellt und gepflegt werden kann. Die nächste Abbildung zeigt den Strukturierungsvorschlag im Überblick. Sie enthält alle wesentlichen Bestandteile und kann an die unterschiedlichen Anforderungen einer Organisation angepasst werden. Im Folgenden werden die einzelnen Dokumentationsbestandteile differenziert betrachtet und kurz erläutert.

Strukturierungsvorschlag: Dokumentation nach DSVO

Stammordner:
(Standort nach Verantwortlichkeit)

1

00 Übersicht
01 Dokumentations-Leitfaden
02 Dokumentation Informationstechnik
03 Dokumentation Sicherheitsmaßnahmen
04 Dokumentation Restrisiko
05 Verfahrensverzeichnis
06 Dienstanweisungen

2

3

Mögliche Dokumentationsmodule:

- Technische und organisatorische Maßnahmen
- Dokumentation Datenschutzmanagement
- Dokumentation von Verschlüsselungsmechanismen
- Dokumentation von Protokollierungsmechanismen
- Sicherheitsmaßnahmen bei Auftragsdatenverarbeitung

Mögliche Dokumentationsmodule:

- Dokumentation des Verfahrenszwecks
- Dokumentation IT-Geräte
- Dokumentation Programme
- Netzplan
- Dokumentation technischer/organisatorischer Vorgaben
- Dokumentation von Auftragsdatenverarbeitung

4

5

Verfahren A, Hinweis auf Verfahrensakte (z. B. Aktenzeichen)
Verfahren B, Hinweis auf Verfahrensakte (z. B. Aktenzeichen)
Verfahren C, Hinweis auf Verfahrensakte (z. B. Aktenzeichen)

Hinweis auf Systemakte (z. B. Aktenzeichen)

Verfahrensakten

Verfahrensakte A

Verfahrensakte B

Verfahrensakte C

Systemakten

Systemakte 1

Systemakte 2

Systemakte 3

Mögliche Inhalte:

00 Übersicht, Datenschutzmanagement
01 Verfahrensbeschreibung
02 Dokumentation der Berechtigungen (User, Administrator)
03 Test, Freigabe
04 Verträge, Auftragsdatenverarbeitung
05 Anlagen

Laufende Verfahrensdokumentation:
– mit einem weiteren Gliederungspunkt innerhalb der Verfahrensakten oder
– ausgegliedert (in einer Akte oder elektronisch - Verweis in der Dokumentation!)

Mögliche Inhalte:

00 Übersicht, Datenschutzmanagement
01 Systembeschreibung
02 Dokumentation der Berechtigungen (User, Administrator)
03 Dokumentation der Datensicherung
04 Verträge, Auftragsdatenverarbeitung
05 Anlagen

Laufende Verfahrensdokumentation:
– mit einem weiteren Gliederungspunkt innerhalb der Verfahrensakten oder
– ausgegliedert (in einer Akte oder elektronisch - Verweis in der Dokumentation!)

1. Einleitung

Eine Dokumentation von automatisierten Verfahren umfasst die folgenden drei Säulen:

1. Dokumentation der IT-Technik
2. Dokumentation der Sicherheitsmaßnahmen
3. Dokumentation der Test- und Freigabeverfahren

Als Erinnerung: Ein automatisiertes Verfahren ist ein Arbeitsablauf mit Hilfe von informationstechnischen Geräten, Programmen und automatisierten Dateien.

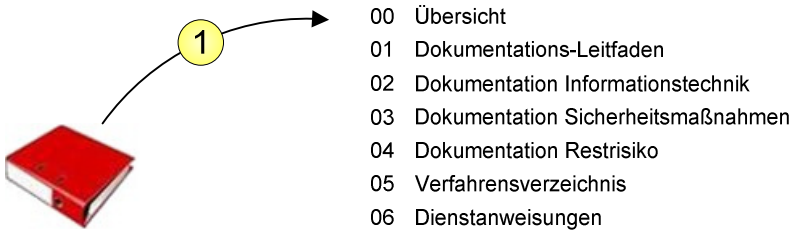
Demnach berücksichtigt die Dokumentation von automatisierten Verfahren gemäß LDSG und DSVO nicht nur die Dokumentation der einzelnen Verfahren an sich, sondern auch die der allgemeinen Informationstechnik (IT), die den entsprechenden Verfahren zu Grunde liegt.

Mit der Dokumentation wird ein System zur Gewährleistung der Transparenz eingeführt. Sie beschreibt, wie die Organisation arbeitet, wenn das System implementiert ist, und wie es Datenschutz und Datensicherheit gewährleistet. Um sicherzugehen, dass die Informationstechnik, die Programme und organisatorischen Regelungen die notwendigen Voraussetzungen erfüllen, werden Prozesse, Zeitpläne, Kontrollen usw. definiert.

Der Anspruch auf Transparenz bedingt weiterhin, dass die Dokumentation als Ganzes übersichtlich und strukturiert aufgebaut und nach definierten Grundsätzen gepflegt wird.

2. Stammordner

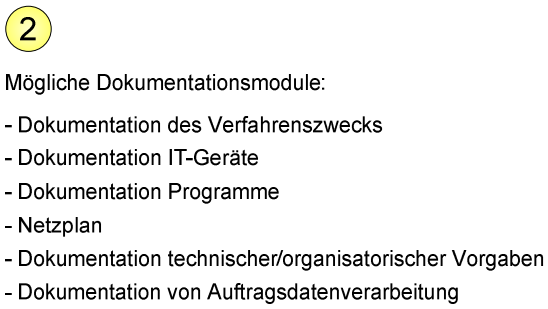
Die Grundlage für eine modulare, übersichtliche und leicht zu erweiternde Dokumentationsstruktur bildet ein übergeordneter Ordner, der die allgemeinen Konzepte, Verzeichnisse und Anweisungen enthält. Dieser „Stammordner“ verweist in seinen einzelnen Gliederungspunkten auf eventuell vorhandene speziellere Dokumentationen.



- Der Dokumentations-Leitfaden ist ein Dokument, das beschreibt, wie die Dokumentation strukturiert ist, aus welchen Bestandteilen eine Dokumentation besteht, wer für was verantwortlich (Datenschutzmanagement) ist usw.

- Die Dokumentation des Einsatzes der Informationstechnik stellt die erste der drei Säulen der Verfahrensdokumentation dar. § 3 Absatz 2 DSVO gibt genaue Hinweise darauf, was dokumentiert werden muss, ohne eine bestimmte Form vorzuschreiben. Bei einem stark modularen Aufbau kann sich folgendes Vorgehen anbieten:

  In einem beschreibenden Dokument wird die Daten verarbeitende Stelle mit ihren Aufgabenbereichen und den zur Aufgabenerfüllung benötigten automatisierten Verfahren und der benötigten IT-Technik darstellt. Dieses Dokument soll einen Überblick über den Aufgabenbereich der Daten verarbeitenden Stelle geben, ohne gleich alle Dokumentations-Bestandteile des § 3 Absatz 2 DSVO zu enthalten. Es stellt das zentrale Dokument dar, das im Stammordner vorgehalten wird und das auf weitere Dokumentations-Module verweist (die dann die geforderten Bestandteile des § 3 Absatz 2 DSVO vervollständigen). Diese Dokumentations-Module (einige mögliche Module sind auf der Abbildung benannt – siehe auch Abbildung unten) können je nach Dokumentationsstruktur bzw. Verantwortlichkeit, im Stammordner oder in anderen Dokumentationsakten (z. B. in den nachfolgend beschriebenen Verfahrens- und Systemakten) geführt werden.

- Die „Dokumentation der Sicherheitsmaßnahmen“ stellt die zweite der drei Säulen der Verfahrensdokumentation dar. In ihr werden die technischen und organisatorischen Maßnahmen beschrieben, die gemäß der §§ 5, 6 und 8 LDSG getroffen werden. Da in der „Dokumentation des Einsatzes der Informationstechnik“ alle relevanten informationstechnischen Geräte und Programme zur Verarbeitung personenbezogener Daten beschrieben sind, ist es sinnvoll, bei der Beschreibung der Sicherheitsmaßnahmen auf diese Dokumentation Bezug zu nehmen. Die Grundlage der Dokumentation der Sicherheitsmaßnahmen bildet eine Risikoanalyse, die die Erforderlichkeit und Angemessenheit der Maßnahmen unter Berücksichtigung der tatsächlichen örtlichen und personellen Gegebenheiten dokumentiert. Welche Gefährdungen und welche weiteren Maßnahmen berücksichtigt werden müssen, beschreibt § 4 DSVO. Auch bei der Dokumentation der Sicherheitsmaßnahmen kann auf zusätzliche Dokumentations-Module verwiesen werden (einige mögliche Dokumentationsmodule sind in der Abbildung und unterhalb dieses Aufzählungspunktes abgebildet), die je nach Dokumentations-Struktur entweder im Stammordner oder

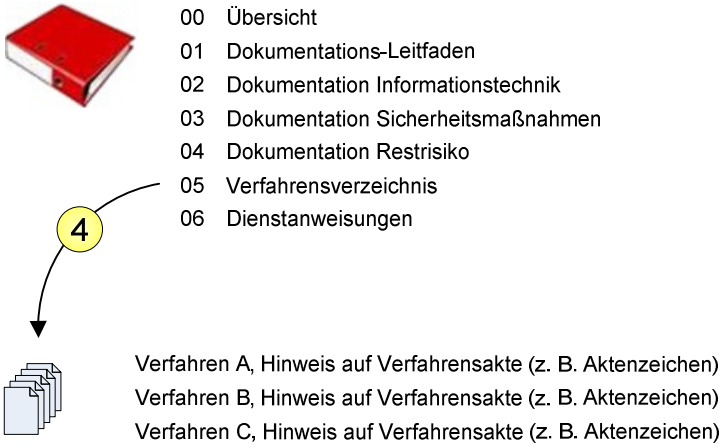
in anderen Dokumentations-Akten (z. B. in den nachfolgend beschriebenen Verfahrens- und Systemakten) geführt werden können.

Mögliche Dokumentationsmodule:

- Technische und organisatorische Maßnahmen
- Dokumentation Datenschutzmanagement
- Dokumentation von Verschlüsselungsmechanismen
- Dokumentation von Protokollierungsmechanismen
- Sicherheitsmaßnahmen bei Auftragsdatenverarbeitung

- Die Restrisiko-Dokumentation ist Bestandteil der „Dokumentation der Sicherheitsmaßnahmen“. In der oben beschriebenen Risikoanalyse werden alle Sicherheitsrisiken – basierend auf der Verfahrensdokumentation – beschrieben und bewertet. Kann den Risiken mit entsprechenden technischen und organisatorischen Maßnahmen entgegengewirkt werden, dann werden sie in der Risikoanalyse dokumentiert. Gibt es für Risiken keine geeigneten Maßnahmen, so müssen diese in der Restrisiko-Dokumentation erläutert werden. Die Restrisiko-Dokumentation kann als Verschlusssache „VS - Nur für den Dienstgebrauch“ eingestuft werden.
- Das Verfahrensverzeichnis nach § 7 LDSG listet alle automatisierten Verfahren einer Organisation auf und soll die Transparenz und Öffentlichkeit dieser Verfahren sicherstellen. Weitere Hinweise zum Verfahrensverzeichnis folgen im nächsten Abschnitt.
- Dienstanweisungen werden nicht explizit im Gesetz erwähnt, runden aber den konzeptionellen Bereich in Verbindung mit der praktischen Umsetzung ab. In den Dienstanweisungen werden die Sicherheitsmaßnahmen, die im Sicherheitskonzept festgelegt sind, für die Mitarbeiter formuliert. Die Dienstanweisungen sollen die Mitarbeiter über alle für sie wichtigen Sicherheitsmaßnahmen am Arbeitsplatz (konventionell und automatisiert) informieren.

3. Erstellung eines Verfahrensverzeichnisses



Das Verfahrensverzeichnis soll die Transparenz und Öffentlichkeit aller automatisierten Verfahren einer Organisation sicherstellen. Häufig beginnen die Schwierigkeiten aber schon bei der Abgrenzung der automatisierten Verfahren untereinander. Deshalb soll an dieser Stelle zunächst eine Möglichkeit zur Verfahrensabgrenzung vorgestellt werden, bevor auf die Strukturierung eingegangen wird.

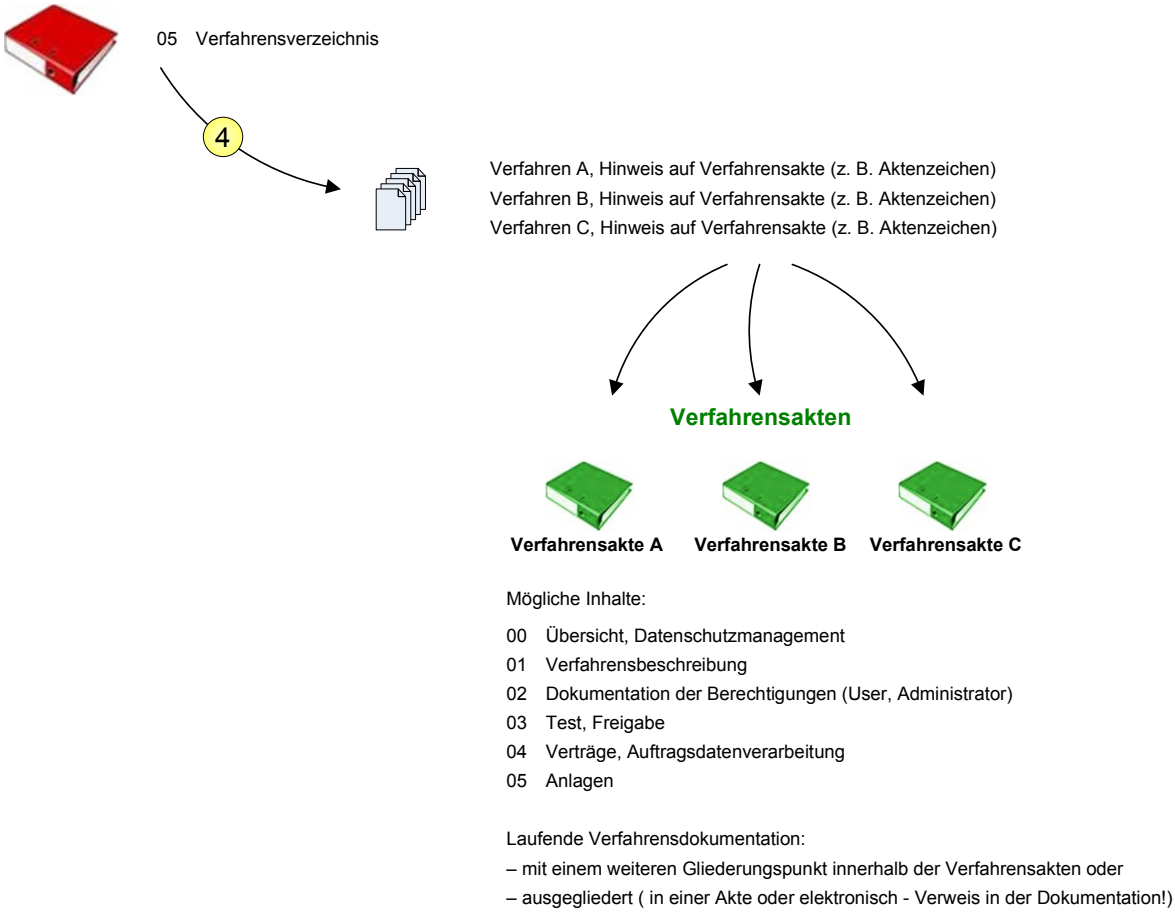
Ein automatisiertes Verfahren ist eine Verwendung von Daten zu einem bestimmten Zweck mit Unterstützung von informationstechnischen Geräten (Hardware) und Computerprogrammen (Software), eingebunden in einem organisatorischen Regelwerk. In dieser Definition finden sich prinzipiell schon alle Komponenten wieder, die im „Stammordner“ (s.o.) dokumentiert wurden. Nun müssen diese Komponenten „nur“ noch untereinander abgegrenzt werden. Die folgende Arbeitsanweisung unten stellt eine mögliche Vorgehensweise vor:

Arbeitsanweisung:

- *Wenn Sie die automatisierten Verfahren ermitteln möchten, überlegen Sie im ersten Schritt zunächst, für welche Zwecke Ihre Organisation Daten verarbeitet. Die Benennung des Datenverarbeitungszwecks ist die Grundlage zur Identifizierung eines automatisierten Verfahrens.*
- *Legen Sie weiterhin eine Liste aller Fachverfahren und Softwareprodukte an.*
- *Weisen Sie nun den entsprechenden Fachverfahren bzw. Softwareprodukten die definierten Datenverarbeitungszwecke zu. Betrachten Sie dabei zunächst die großen Fachverfahren, wie z. B. die Fachverfahren „Verwaltung von Einwohnermeldedaten“ oder „Kommunale Finanzverwaltung“, die zu einem ganz speziellen Zweck eingesetzt werden und sich deshalb gut von den anderen Verfahren abgrenzen lassen.*

- *Danach bleiben auf der Liste in der Regel nur noch die allgemeinen Textverarbeitungsprogramme oder die administrativen Tools stehen. Überlegen Sie, zu welchem definierten Verarbeitungszweck die Programme eingesetzt werden. Vielleicht lassen sich die Programme auch zusammenfassen und einem Verarbeitungszweck zuweisen, z. B. die Standardsoftwareprodukte Word und Excel zu einem Verarbeitungszweck „Bürokommunikation“.*

4. Verfahrensakten



Die Abgrenzung der automatisierten Verfahren untereinander ist der aufwändigste Anteil zur Erstellung eines Verfahrensverzeichnisses. Nun bleibt noch die Aufgabe, die automatisierten Verfahren in einer übersichtlichen Struktur zu dokumentieren. Wie oben schon erwähnt, wird in diesem Strukturierungsvorschlag im „Stammordner“ ein Verfahrensverzeichnis in Form einer Auflistung der gesetzlich vorgeschriebenen Angaben (§ 7 LDSG) geführt. Diese Auflistung schafft aufgrund ihrer Kürze einen hohen Grad an Übersichtlichkeit und dient als eine Art „Zusammenfassung“, das den Verweis (Aktenzeichen) auf die ausführliche Dokumentation liefert. Denn: das Verfahrensverzeichnis ersetzt nicht die Verfahrensdokumentation.

Betrachtet man insbesondere die großen automatisierten Verfahren, z. B. „Verarbeitung von Einwohnermeldedaten“, dann fallen für die entsprechenden Fachverfahren viele Dokumentationsunterlagen z. B. Administrationshandbücher, Dokumentationen zu Sicherheitspatches und Softwareupdates, Konzepte für die Rechtevergabe usw. an. Damit diese Dokumentationsunterlagen den entsprechenden Verfahren zugeordnet werden können, ist es empfehlenswert, für die einzelnen automatisierten Verfahren Verfahrensakten anzulegen und mit Aktenzeichen zu kennzeichnen. Diese Aktenzeichen werden im Verfahrensverzeichnis, evtl. auch mit einem Hinweis auf den Standort der Verfahrensakten, vermerkt. So lässt sich im Verfahrensverzeichnis mit einem Blick nachvollziehen, wo die entsprechende Verfahrensdokumentation zu finden ist.

In die Verfahrensakte werden nun systematisch alle notwendigen Konzepte und Dokumentationen aufgenommen, dabei kann die oben dargestellte Gliederung bei jedem Verfahren unterschiedlich umfangreich ausfallen. Grundsätzlich werden in den Verfahrensakten immer dann Konzepte, Verträge o. ä. aufgenommen, wenn sie sich speziell auf das Verfahren beziehen und nicht durch die allgemeine Dokumentation im „Stammordner“ abgedeckt werden. So gehören in diesem Strukturierungsvorschlag u. a. Test und Freigabe (als dritte Säule der Verfahrensdokumentation), die verfahrensspezifisch für jedes automatisierte Verfahren durchgeführt bzw. erteilt werden, in die Verfahrensakte.

5. Systemakten

Mögliche Inhalte:

00 Übersicht, Datenschutzmanagement
01 Systembeschreibung
02 Dokumentation der Berechtigungen (User, Administrator)
03 Dokumentation der Datensicherung
04 Verträge, Auftragsdatenverarbeitung
05 Anlagen

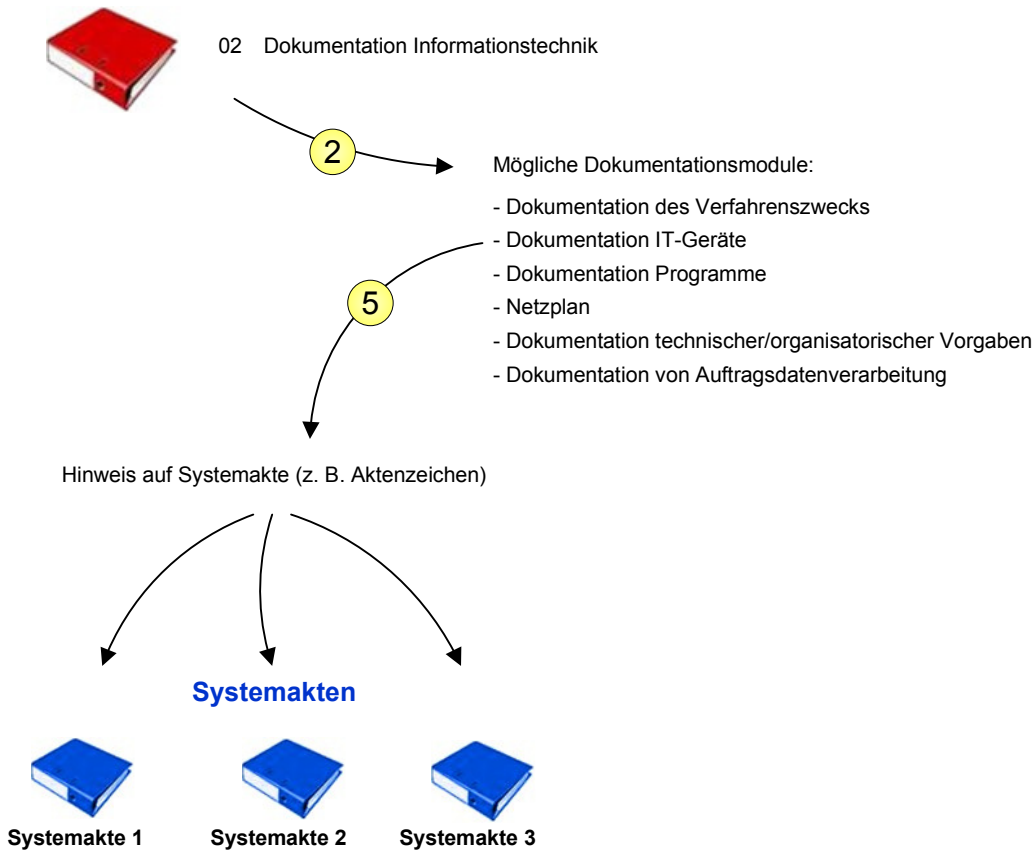
Laufende Verfahrensdokumentation:
– mit einem weiteren Gliederungspunkt innerhalb der Verfahrensakten oder
– ausgegliedert (in einer Akte oder elektronisch - Verweis in der Dokumentation!)

Die Dokumentation der eingesetzten Hardwareausstattung und Basissoftware (Betriebssysteme, Datenbanksysteme, Datensicherungssysteme usw.) wurde bei der Beschreibung der Verfahrensakten bewusst noch nicht angesprochen. Es ist auch nicht sinnvoll, diese Dokumentation in die Verfahrensakten aufzunehmen, da vielfach ein System an mehreren Verfahren beteiligt ist. Das würde zur Unübersichtlichkeit und zu Redundanzen führen. Daher wer-

den in diesem Strukturierungsvorschlag die eingesetzten Systeme in Systemakten dokumentiert. Diese Systemakten werden so unterschiedlich sein, wie die Systeme, die dokumentiert werden. Eine Systemakte für einen Domänencontroller oder Datenbankserver wird anders aussehen als eine Systemakte für einen PC-Arbeitsplatz, daher kann der oben beschriebene Gliederungsvorschlag nur eine Leitlinie darstellen.

In eine Systemakte gehören alle die Konzepte, Verträge o. ä., die sich speziell auf das System beziehen und nicht durch die allgemeine Dokumentation im „Stammordner“ abgedeckt werden. So können z. B. die speziellen Berechtigungen, die ein Systemadministrator an einem Datenbankserver besitzt, in der Systemakte des Datenbankservers dokumentiert werden. Doch auch die laufende Dokumentation nimmt einen hohen Stellenwert beim Führen der Systemakte ein, z. B. das regelmäßige Protokoll zur Durchführung einer Datensicherung.

Wie werden die Systemakten jetzt in die bestehende Dokumentations-Struktur integriert?



Im § 3 Abs. 2 Nr. 2 DSVO wird im Zusammenhang mit der „Dokumentation des Einsatzes der Informationstechnik“ die Dokumentation der für die Verfahren verwendeten informationstechnischen Geräte verlangt. Das kann im einfachsten Fall ein eigenes Verzeichnis in Form einer Tabelle sein oder die Geräte werden im Inventarverzeichnis mit aufgenommen. In

diesem Strukturierungsvorschlag wird die Dokumentation der informationstechnischen Geräte um einen Verweis (z. B. das Aktenzeichen der jeweiligen Systemakte) ergänzt. Somit wird das Verzeichnis der informationstechnischen Geräte im „Stammordner“ geführt (bzw. auf ein Inventarverzeichnis, z. B. auch in elektronischer Form verwiesen) und die detaillierte Systemdokumentation befindet sich in den jeweiligen Systemakten.

6. Was wird mit der vorgestellten Struktur erreicht?

Der vorgestellte Gliederungsvorschlag orientiert sich an einem hierarchischen modularen System, dass sowohl für einen Prüfer oder Auditor als auch für den Systemverantwortlichen und alle an der Dokumentation beteiligten Personen ein hohes Maß an Übersichtlichkeit, Strukturierung und Flexibilität liefert. So ist im „Stammordner“ auf einem Blick sowohl der organisatorische und technisch-organisatorische Aufbau einer Organisation ersichtlich als auch ein Überblick über die datenschutzkonforme Dokumentation entsprechend LDSG und DSVO gegeben. Für nähere Informationen zu einem bestimmten Verfahren oder System kann dann entsprechend der vermerkten Verweise (Aktenzeichen), auf die spezielleren Dokumentationen in den Verfahrens- bzw. Systemakten zurückgegriffen werden.

Die Struktur der Dokumentation kann abgeändert bzw. erweitert werden, um sie an die unterschiedlichen Organisationen anzupassen. Es sollte jedoch darauf geachtet werden, dass die Dokumentation nicht zu stark in Module aufgeteilt wird, da ansonsten die Übersichtlichkeit, die eigentlich erreicht werden soll, verloren gehen kann.

Für weitere Fragen stehe ich gerne zur Verfügung:

Angelika Martin
uld34@datenschutzzentrum.de
Tel.: 0431/988-1280