DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ
BADEN-WÜRTTEMBERG

Hinweise
zum
Verfahrensverzeichnis

Stand: 1. März 2006

Der Landesbeauftragte für den Datenschutz in Baden-Württemberg
Urbanstraße 32
70182 Stuttgart
Telefon 0711/615541-0
Telefax 0711/615541-15
E-Mail: poststelle@lfd.bwl.de
(Schutzbedürftige Daten sollten nicht unverschlüsselt per E-Mail oder via Telefax übertragen werden.)
PGP-Fingerprint: A5A5 6EC4 47B2 6287 E36C 5D5A 43B7 29B6 4411 E1E4
Homepage: www.baden-wuerttemberg.datenschutz.de

Inhaltsverzeichnis

---

1. Allgemeines

Nach § 11 des Landesdatenschutzgesetzes (LDSG) muss jede öffentliche Stelle des Landes ein Verzeichnis der automatisierten Verfahren führen, mit denen sie personenbezogene Daten verarbeitet. Welche Angaben in dieses Verfahrensverzeichnis aufzunehmen sind, ist durch die gesetzliche Regelung im Einzelnen festgelegt. Gleichwohl ergeben sich in der Praxis immer wieder Fragen und Unklarheiten zum Inhalt. Leider erweisen sich die Verfahrensverzeichnisse immer wieder als wenig aussagekräftig oder unvollständig. Ziel dieses Merkblattes ist daher, Hinweise zur Erstellung des Verfahrensverzeichnisses zu geben.

2. Welchen Nutzen hat das Verfahrensverzeichnis?

Im Verfahrensverzeichnis muss die Daten verarbeitende Stelle dokumentieren, welche personenbezogenen Daten sie mit Hilfe welchen automatisierten Verfahren auf welche Weise verarbeitet und welche Datenschutzmaßnahmen sie dabei getroffen hat. Es ermöglicht ihr folglich, den Überblick über ihre Datenverarbeitung zu bewahren. Das Verfahrensverzeichnis ist somit unverzichtbar für eine effektive Eigenkontrolle. Zudem ist es eine wichtige Informationsquelle für Fremdkontrollen, etwa datenschutzrechtliche Kontrollen durch meine Dienststelle.

3. Was ist ein automatisiertes Verfahren?

Unklarheiten können sich bereits bei der Frage ergeben, was unter einem automatisierten Verfahren zu verstehen ist. Zum Teil trägt bereits das Landesdatenschutzgesetz selbst zur Klärung bei. Nach § 11 Abs. 2 LDSG sind zu jedem automatisierten Verfahren unter anderem die Zweckbestimmung und die Rechtsgrundlage der Verarbeitung anzugeben. Ein automatisiertes Verfahren umfasst demzufolge sämtliche Programme oder Programmteile, mit denen die Daten verarbeitende Stelle personenbezogene Daten aufgrund einer bestimmten Rechtsgrundlage für einen bestimmten Zweck verarbeitet.

Schwierigkeiten ergeben sich in der Praxis immer wieder bei Dateien, die die Daten verarbeitende Stelle mit Hilfe von Bürokommunikations-Programmen wie etwa einem Textverarbeitungs- oder Tabellenkalkulationsprogramm erstellt. Folgende Fragen ergeben sich: Ist das Bürokommunikations-Programm ein automatisiertes Verfahren? Sind das Bürokommunikations-Programm zusammen mit den damit erzeugten Dateien automatisierte Verfahren? Oder liegt überhaupt kein automatisiertes Verfahren vor? Das bereits Ausgeführte liefert die Antwort: Kennzeichnend für ein automatisiertes Verfahren ist die Verarbeitung personenbezogener Daten für einen bestimmten Zweck. Ein Bürokommunikations-Programm, für sich allein betrachtet, kann daher kein automatisiertes Verfahren sein, weil kein Bezug zur Verarbeitung personenbezogener Daten besteht. Im Gegensatz dazu sind aber das Bürokommunikations-Programm und eine oder mehrere damit erstellte Dateien, mit denen personenbezogene Daten für einen bestimmten Zweck verarbeitet werden, ein automatisiertes Verfahren. Ein automatisiertes Verfahren ist damit beispielsweise eine mit Hilfe des Tabellenkalkulationsprogramms Excel erstellte Datei aller von einem Landratsamt zu überwachenden Tankstellenbetreiber.

4. Welche Datenverarbeitungen sind zu dokumentieren?

Die verantwortliche Stelle muss im Verfahrensverzeichnis Angaben zu sämtlichen von ihr betriebenen automatisierten Verfahren machen, mit denen sie personenbezogene Daten verarbeitet. Von der Dokumentationspflicht ausgenommen sind nach § 11 Abs. 3 LDSG nur solche automatisierte Verfahren,

- deren einziger Zweck die Information der Öffentlichkeit ist sowie
- Verfahren für allgemeine Verwaltungszwecke (z. B. Verfahren der Textverarbeitung).

Auch wenn keine Dokumentationspflicht besteht, muss die Stelle nach Maßgabe des § 9 LDSG Datenschutzvorkehrungen treffen. So muss sie etwa bei der Textverarbeitung regeln, wann welche Texte mit personenbezogenem Inhalt zu löschen sind.

5. Welche Angaben sind in das Verfahrensverzeichnis aufzunehmen?

Der Gesetzgeber hat in § 11 Abs. 2 LDSG festgelegt, welche Angaben im Einzelnen in das Verfahrensverzeichnis aufzunehmen sind. Diese Bestandteile des Verfahrensverzeichnisses sollen im Folgenden erläutert werden:

- *Name und Anschrift der verantwortlichen Stelle*
  Die verantwortliche Stelle ist nach § 3 Abs. 3 LDSG die Stelle, die personenbezogene Daten für sich selbst verarbeitet oder durch andere im Auftrag verarbeiten lässt.

- *Die Bezeichnung des Verfahrens*
  Das Verfahren ist eindeutig zu bezeichnen. Über die Bezeichnung muss sich das Verfahren im DV-System der verantwortlichen Stelle oder eines beauftragten Auftragnehmers identifizieren lassen.
  Mitunter kommt es vor, dass Verfahren als „Liste“ oder „Datei“ bezeichnet werden, wobei nicht erkennbar ist, ob der Begriff „Datei“ edv-technisch gemeint ist, das gemeldete Verfahren also beispielsweise lediglich aus einer Word- oder Excel-Datei besteht, oder ob das Verfahren beispielsweise trotz der Bezeichnung als "Datei" als datenbankbasierte Fachanwendung programmiert wurde. Um Missverständnisse zu vermeiden, sollten zumindest datenbankbasierte Fachanwendungen nicht als "Liste" oder "Datei" bezeichnet werden.

- *Die Zweckbestimmung und die Rechtsgrundlage der Verarbeitung*
  Der Zweck der Datenverarbeitung ist so präzise wie möglich zu benennen.
  Nach § 4 Abs. 1 LDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn das Landesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene, d.h. die Person, deren Daten verarbeitet werden sollen, eingewilligt hat. Im Verfahrensverzeichnis ist daher zu dokumentieren, ob die Verarbeitung aufgrund einer Einwilligung oder aufgrund einer Rechtsvorschrift erfolgt. Erfolgt die Verarbeitung aufgrund einer Rechtsvorschrift, so ist sie zusammen mit den einschlägigen Paragraphen präzise anzugeben.

- *Die Art der gespeicherten Daten*
  Hier geht es nicht darum, jedes einzelne im automatisierten Verfahren gespeicherte Datenfeld aufzuführen. Vielmehr sind sachlich zusammengehörende Datenfelder zu sinnvollen Gruppen zusammenzufassen und diese Datenarten dann allgemein verständlich zu benennen. Beispiele dafür sind:
  - Ordnungsmerkmal (z. B. eine Personennummer)
  - Familienname
  - Vorname
  - Geburtstag
  - Zahl der Kinder
  - Kfz-Kennzeichen
  - Jahreseinkommen

  Einzelmerkmale wie etwa "Postleitzahl", "Wohnort", "Straße" und "Hausnummer" können dabei zu einem Sammelmerkmal, in diesem Falle "Postanschrift", zusammengefasst werden. Bei der Bildung von Sammelmerkmalen ist allerdings darauf zu achten, dass diese noch aussagekräftig bleiben. Die Kunst besteht also darin, den richtigen Konkretisierungsgrad zu finden. Einerseits dürfen die Begriffe, die die Art der gespeicherten Daten beschreiben, nicht zu allgemein sein, weil sonst die Transparenz über den Umfang der Datenspeicherung verloren ginge. Die Aussagekraft von Begriffen wie "Personalien" oder "Vermögensverhältnisse" wäre recht begrenzt. Andererseits sollten die gewählten Begriffe so flexibel sein, dass nicht jede kleine Änderung am automatisierten Verfahren eine Änderung am Verfahrensverzeichnis nach sich zieht.

- *Der Kreis der Betroffenen*
  Betroffene sind die natürlichen Personen, deren Daten mit Hilfe des automatisierten Verfahrens verarbeitet werden. Der Kreis der Betroffenen ist so präzise wie möglich zu bezeichnen. So wäre etwa die Angabe "natürliche Personen" bei einem computergestützten Ausleihsystem einer Bibliothek viel zu allgemein. In diesem Fall lässt sich der Kreis der Betroffenen wesentlich genauer angeben, z. B. "alle Personen, die einen Leseausweis haben".

- *Die Empfänger der Daten oder Gruppen von Empfängern sowie die jeweiligen Datenarten, wenn vorgesehen ist,*
  a) die Daten zu übermitteln,

b) sie innerhalb der öffentlichen Stelle für einen weiteren Zweck zu nutzen oder

c) sie im Auftrag verarbeiten zu lassen.

Empfänger ist nach § 3 Abs. 4 LDSG jede Person oder Stelle, die Daten erhält, mit Ausnahme des Betroffenen. Angaben sind sowohl bei einer Datenweitergabe an einen Dritten (Fall a) als auch bei einer Zweckänderung innerhalb der verantwortlichen Stelle (Fall b) oder bei der Einschaltung eines Auftragnehmers (Fall c) zu machen.

- *Fristen für die Prüfung der Sperrung und Löschung der Daten oder für die Sperrung und Löschung*
  Wer personenbezogene Daten mit Hilfe eines automatisierten Verfahrens verarbeitet, muss - beginnend mit der erstmaligen Speicherung von Daten - festlegen, wann welche Datenarten zu sperren oder zu löschen sind.

- *Die zugriffsberechtigten Personengruppen oder Personen, die allein zugriffsberechtigt sind*
  Zugriffsberechtigte können sowohl Mitarbeiter der öffentlichen Stelle als auch Dritte sein. Nicht notwendig ist, die Zugriffsberechtigten namentlich aufzuführen. Dies würde einen hohen Änderungsbedarf des Verfahrensverzeichnisses nach sich ziehen. Vielmehr können die Zugriffsberechtigten auch funktionsbezogen aufgeführt werden. Eine Bezeichnung, wie z. B. "Mitarbeiter der Personalabteilung", sollte dabei nicht verwendet werden, da sie offen lässt, ob **alle** oder nur bestimmte Mitarbeiterinnen und Mitarbeiter dieser Abteilung zugriffsberechtigt sind. Empfehlenswert sind stattdessen Bezeichnungen wie z. B. "Alle Mitarbeiter der Personalabteilung, die Anträge auf ... bearbeiten". Sofern die zugriffsberechtigten Mitarbeiter auf unterschiedliche Datenarten zugreifen können, sollte auch dies erkennbar sein.

- *Eine allgemeine Beschreibung der eingesetzten Hardware, der Vernetzung und der Software*
  Zu dokumentieren ist die technische Infrastruktur, in der die verantwortliche Stelle ihre automatisierten Verfahren betreibt. Es sind Angaben zur Hardware (z. B. Anzahl der vorhandenen Großrechner, Server und Clients, Angaben zu aktiven Netzkomponenten), der Vernetzung (z. B. Typ und Topologie des lokalen Computernetzwerks wie Ethernet oder Token Ring, Informationen zu den eingesetzten aktiven Netzkomponenten (z. B. Hubs, Switches), zu Anschlüssen an Landes- oder kommunale Netze sowie an das Internet oder andere öffentliche Net-

ze) und der eingesetzten Software (z. B. Betriebssysteme, Datenbanksysteme, Sicherheitssoftware oder andere systemnahe Software wie z. B. Tools zur Fernadministration) zu machen.
Angaben wie "Windows-Netzwerk" oder "Stand-alone-PC" allein reichen nicht aus, um die EDV-technische Infrastruktur zu beschreiben. Da sich die einzelnen Windows-Varianten in sicherheitstechnischer Hinsicht ganz erheblich unterscheiden, ist die Angabe "Windows" zur Beschreibung des Betriebssystems unzureichend. Die Beschreibung sollte in jedem Fall erkennen lassen, welches Betriebssystem auf wie vielen der eingesetzten Clients, Server sowie etwa vorhandenen unvernetzten PC eingesetzt wird.

- *Die technischen und organisatorischen Maßnahmen*
  Nach § 9 LDSG muss die verantwortliche Stelle technische und organisatorische Sicherheitsmaßnahmen treffen, um eine datenschutzgerechte Verarbeitung personenbezogener Daten sicherzustellen. Diese Maßnahmen muss sie in ihrem Verfahrensverzeichnis beschreiben. Unzureichend wäre, wenn das Verfahrensverzeichnis lediglich Aufschluss darüber geben würde, in welchen der in § 9 Abs. 3 LDSG genannten Kontrollbereiche (Zutrittskontrolle, Datenträgerkontrolle, Speicherkontrolle etc.) Maßnahmen getroffen sind. Eine solche Art der Dokumentation ist wenig aussagekräftig. Vielmehr hat die verantwortliche Stelle in angemessener Form darzustellen, welche Sicherheitsmaßnahmen sie denn konkret umgesetzt hat. Folgende beispielhaft erwähnte Aspekte mögen verdeutlichen, welche Detaillierung dabei empfehlenswert ist:
  - Unzulänglich wäre etwa, wenn beispielsweise im Zusammenhang mit den Maßnahmen der Zugriffskontrolle, die einen unberechtigten Zugriff auf personenbezogene Daten verhindern sollen, nur Stichwörter wie "Passwortschutz", "differenzierte Zugriffsberechtigungen" oder "Dienstanweisung" genannt würden. Diese Maßnahmen sind zwar allesamt notwendig, jedoch sind dafür unterschiedlichste Realisierungsmöglichkeiten vorstellbar, die letztlich ein ganz unterschiedliches Sicherheitsniveau gewährleisten. Es muss daher erkennbar sein, **wie** die Realisierung jeweils erfolgt.
  - Im Hinblick auf den Passwortschutz sollten beispielsweise die im Betriebssystem eingestellten Passwortkonventionen wie Mindestlänge, Höchstalter, Sperrung nach wie viel Fehlversuchen oder Passwort-Historie im Einzelnen bezeichnet werden (etwa durch Screen-Shots). Auch im Hinblick auf weitere Gestaltungsmöglichkeiten des Passwortschutzes, die etwa in unserem Merkblatt zum Umgang mit Passwörtern beschrieben sind, vgl.

http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/Umgang-mit-Passwörtern.pdf,

sollte dargestellt werden, welche Optionen in den jeweiligen Installationen gewählt wurden und welche Anforderungen an Passwörter technisch und welche organisatorisch sichergestellt werden.

- Im Hinblick auf die Zugriffsberechtigungen sollte beispielsweise angegeben werden, welches Filesystem genutzt wird (z. B. NTFS). In Abhängigkeit vom Datenhaltungskonzept sollte dargelegt werden, wer Zugriff auf welche Verzeichnisse erhält (z. B. individuelle Ablagen, Ablagen für Gruppenverzeichnisse, Ablagen für Daten der Anwendungsprogramme).
- Es sollte erkennbar sein, ob und, wenn ja, wofür Verzeichnisfreigaben (Shares) verwendet werden. Gegebenenfalls sollte dargestellt werden, dass deren Nutzung an den einzelnen Arbeitsplatz-PC durch eine entsprechende Systemkonfiguration unterbunden wird.
- Soweit die Anwendungsprogramme sicherheitsrelevante Funktionen bieten (z. B. eigenen Passwortschutz oder eigene Zugriffsberechtigungsverwaltung und -steuerung), ist auch darauf einzugehen und zu beschreiben, ob und, wenn ja, wie diese Funktionen genutzt werden.
- Auch im Hinblick auf weitere, sicherheitsrelevante Einstellungen der Betriebssysteme und Anwendungsprogramme sollte, beispielsweise mit Hilfe von Screen-Shots, angegeben werden, wie davon Gebrauch gemacht wird.
- Was etwa geplante Fernsteuerungs- und Fernwartungsmaßnahmen betrifft, so sollte erwähnt werden, wie dieser Zugriff jeweils erfolgen soll (z. B. über Landesverwaltungsnetz, ISDN-Wählverbindung oder über Internet). Je nachdem, welcher Weg dafür gewählt wird, ist darzustellen, welche sicherheitsrelevanten Parameter und welche sonstigen Schutzmaßnahmen dafür gewählt werden (z. B. Option zur Einwahl von außen deaktiviert) und auf welche Weise die Systemverantwortlichen vor Ort jeweils mitwirken müssen, um die Verbindung aufzubauen. Näheres zum datenschutzgerechten Einsatz von Fernsteuerungssoftware ist unserem Merkblatt unter

  http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/Einsatz-von-Fernsteuerungssoftware.pdf

  zu entnehmen.
- Im Zusammenhang mit der Anbindung beispielsweise an das Landesverwaltungsnetz, das Netz eines Regionalen Rechenzentrums oder ein öffentliches Netz wie das ISDN-Netz oder das Internet ist darzustellen, wie diese Netzan-

bindung gesichert und beispielsweise ein unberechtigter Verbindungsaufbau verhindert wird.
- Sofern über die lokalen Netze auch E-Mails ausgetauscht oder im Internet gesurft werden soll, sind auch die dafür vorgesehenen Sicherheitsmaßnahmen zu beschreiben.

Da in aller Regel eine Vielzahl von Sicherheitsmaßnahmen nicht vom eingesetzten automatisierten Verfahren, sondern von der zu Grunde liegenden technischen Infrastruktur abhängen (z. B. Sicherheitsmaßnahmen, die im lokalen Computernetzwerk getroffen sind), empfiehlt es sich, diese verfahrensunabhängig getroffenen Sicherheitsmaßnahmen in einem Datenschutz- und Datensicherheitskonzept gebündelt zu beschreiben. Im Verfahrensverzeichnis kann dann auf dieses Konzept verwiesen werden. Wichtig ist dabei dann, dass die Inhalte, auf die verwiesen wird, konkret bezeichnet werden, also z. B. einzelne Gliederungsnummern oder Kapitel von genau (d. h. Angabe von Titel und Version/Stand) bezeichneten Dokumenten.

Die hier genannten Punkte können nur beispielhaft für Fragestellungen stehen, die im Verfahrensverzeichnis zu berücksichtigen sind. Je nach der Nutzungssituation vor Ort kann die Behandlung weiterer Punkte im Verfahrensverzeichnis erforderlich sein. Weitere in Frage kommende Maßnahmen finden sich etwa in unseren Merkblättern
- zum Einsatz von PC und lokalen Netzwerken *http://www.baden-wuerttemberg.datenschutz.de/datensicherheit-beim-einsatz-von-pc-und-lokalen-netzwerken-allgemeine-hinweise/*
- zur Fernsteuerung *http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/Einsatz-von-Fernsteuerungssoftware.pdf* oder
- zum Thema Internet und Datenschutz *http://www.baden-wuerttemberg.datenschutz.de/488-2*.

Ist es im Einzelfall unklar, ob und mit welcher Ausführlichkeit bestimmte Fragestellungen im Verfahrensverzeichnis angesprochen werden sollen, so kann es hilfreich sein, sich in die Rolle eines Lesers zu versetzen, der der öffentlichen Stelle nicht angehört, aber anhand des Verfahrensverzeichnisses darüber informiert werden soll, welche Datenverarbeitungsvorgänge ablaufen, auf welcher Rechtsgrundlage dies erfolgt und ob dafür ausreichende technische und organi-

satorische Schutzmaßnahmen ergriffen wurden.

6. Wer führt das Verfahrensverzeichnis?

Sofern die verantwortliche Stelle einen behördlichen Datenschutzbeauftragten i.S. von § 10 LDSG bestellt hat, gehört es zu dessen Aufgaben, das Verfahrensverzeichnis zu führen (§ 10 Abs. 4 Nr. 3 LDSG). Andernfalls muss die verantwortliche Stelle im Rahmen ihrer Geschäftsverteilung festlegen, welcher Bedienstete für die Führung des Verfahrensverzeichnisses verantwortlich ist. In jedem Falle muss die verantwortliche Stelle durch organisatorische Regelungen sicherstellen, dass der für die Führung des Verfahrensverzeichnisses Verantwortliche von allen automatisierten Verfahren erfährt.

7. Wer kann das Verfahrensverzeichnis einsehen?

Wie bereits ausgeführt, dient das Verfahrensverzeichnis in erster Linie der Eigenkontrolle. Im Rahmen der ihm gesetzlich übertragenen Aufgaben kann auch der Landesbeauftragte für den Datenschutz Baden-Württemberg Einblick in die Verfahrensverzeichnisse der öffentlichen Stellen des Landes nehmen. Schließlich muss die verantwortliche Stelle eine Reihe von Angaben des Verfahrensverzeichnisses auf Antrag jedem in geeigneter Weise verfügbar machen. Ausgenommen von dieser Regelung sind automatisierte Verfahren des Landesamtes für Verfassungsschutz. Keine Einsicht erhalten Interessierte in die Angaben, die die internen Abläufe und Strukturen der Daten verarbeitenden Stelle beschreiben. Dazu gehören Angaben zu den Zugriffsberechtigten, die allgemeine Beschreibung zur technischen Infrastruktur sowie die getroffenen technischen und organisatorischen Sicherheitsmaßnahmen.

8. Weitere Informationen

Weitere Informationen rund um das Thema Datenschutz finden sich im Internetangebot des virtuellen Datenschutzbüros, das von zahlreichen nationalen und internationalen Datenschutzbeauftragten getragen wird, unter

www.datenschutz.de