



DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ
BADEN-WÜRTTEMBERG

Hinweise zum Landesdatenschutzgesetz

Stand: 8. Mai 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	4
2. Bestimmungen im Einzelnen	4
2.1 Der Anwendungsbereich des Gesetzes - § 2	4
2.2 Die Begriffe des Datenschutzgesetzes - § 3	8
2.3 Die Zulässigkeit der Datenverarbeitung - § 4	9
2.4 Die Chipkartenregelung - § 5 Abs. 2	10
2.5 Die Wartung von EDV-Systemen - § 7 Abs. 5	12
2.6 Datenvermeidung und Datensparsamkeit - § 9 Abs. 1	12
2.7 Die Datensicherheit („11 Gebote“) - § 9 Abs. 3	13
2.8 Der behördliche Datenschutzbeauftragte - § 10	13
2.9 Das Verzeichnissverzeichnis - § 11	14
2.10 Die Vorabkontrolle - § 12	15
2.11 Datenerhebung und Videoüberwachung - § 13	16
2.12 Die Unterrichtungspflichten - § 14	17
2.13 Datenspeicherung, -veränderung und -nutzung - § 15	18
2.14 Die Wissenschaftsregelungen - § 19 und § 35	18
2.15 Datenübermittlung ins Ausland - § 20	21
2.16 Das Auskunftsrecht - § 21	22
2.17 Die Berichtigung unrichtiger Daten, Löschung und Sperrung - §§ 22 bis 24	22
2.18 Die Schadensersatzregelung - § 25	23
2.19 Der Landesbeauftragte für den Datenschutz - §§ 26 bis 32	23
2.20 Die personenbezogenen Daten 'besonderer Art' - § 33	24
2.21 Der Personaldatenschutz - § 36	25
3. Ergänzende Informationen	25
3.1 Aktuelle Fassung des Landesdatenschutzgesetzes	25
3.2 Virtuelles Datenschutzbüro	26

1. Allgemeines

Zum 1. September 2000 wurde das Landesdatenschutzgesetz erstmals seit 1991 wieder umfassend geändert (Gesetzblatt für Baden-Württemberg 2000, Seite 450 ff.). Anlass hierfür war die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG L 281 vom 23. November 1995, S. 31, nachfolgend als "EG-Datenschutzrichtlinie" bezeichnet). Die EG-Datenschutzrichtlinie stellt fest, dass das Niveau des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten in den Mitgliedstaaten unterschiedlich sei. Dies hemme Wirtschaftstätigkeiten auf Gemeinschaftsebene, verfälsche den Wettbewerb und hindere die im Anwendungsbereich des Gemeinschaftsrechts tätigen Behörden daran, ihren Auftrag zu erfüllen. Diese Hemmnisse könnten nur durch eine Angleichung der Rechtsvorschriften über die Rechte und Freiheiten von Personen bei der Verarbeitung ihrer persönlichen Daten beseitigt werden. Es müsse innerhalb der Gemeinschaften ein gleichwertiges Schutzniveau hergestellt werden. Dies zu erreichen ist Ziel der EG-Datenschutzrichtlinie. Mit den in Kraft getretenen Änderungen des Landesdatenschutzgesetzes wurden die europarechtlichen Vorgaben in Landesrecht umgesetzt.

Inhaltlich ist das Änderungsgesetz geprägt von dem Bemühen, möglichst wenig am Bestehenden zu ändern. Es beschränkt sich auf solche Änderungen, die aufgrund der EG-Datenschutzrichtlinie zwingend erforderlich waren. Darüber hinaus wurde das Datenschutzrecht nur "punktuell" weiterentwickelt.

Was hat sich nun konkret geändert? Nachfolgend sollen die wesentlichen Bestimmungen kurz dargestellt werden.

2. Bestimmungen im Einzelnen

2.1 Der Anwendungsbereich des Gesetzes - § 2

§ 2 LDSG regelt den Anwendungsbereich des Gesetzes. Obwohl die Bestimmung überwiegend neu gefasst wurde, hat sich im Grunde genommen rechtlich so gut wie nichts geändert.

Bisher galt das Landesdatenschutzgesetz nach § 2 Abs. 1 LDSG auch für die Verarbeitung personenbezogener Daten durch Vereinigungen der dort

angeführten öffentlichen Stellen "ungeachtet ihrer Rechtsform". Nach richtiger Lesart waren damit jedenfalls auch solche vom Land oder von Gemeinden gegründete und beherrschte juristische Personen des Privatrechts (AG, GmbH) gemeint, die der Sache nach Aufgaben der öffentlichen Verwaltung wahrnehmen. Tätig werden diese Unternehmen in der Regel im Bereich der Daseinsvorsorge. Die Gesetzesbegründung nennt insoweit beispielhaft kommunale Versorgungsunternehmen, Krankenhäuser, Wohnungsbauunternehmen und Abfallbeseitigungsgesellschaften. Trotz des eindeutigen Wortlauts der Bestimmung war bisher jedoch immer wieder in Zweifel gezogen worden, dass diese privaten "Beteiligungsgesellschaften" tatsächlich dem gleichen Datenschutzrecht unterliegen wie die öffentlichen Stellen, deren Aufgaben sie wahrnehmen. Mit dem neuen § 2 Abs. 2 LDSG wird dies nun klargestellt. Die "Vereinigungen" werden aus Absatz 1 herausgenommen und stattdessen wird in Absatz 2 fingiert ("gelten"), dass sich auch privatrechtlich organisierte Stellen grundsätzlich nach dem öffentlichen Datenschutzrecht zu richten haben, wenn sie Aufgaben der öffentlichen Verwaltung wahrnehmen und wenn die öffentliche Hand entscheidenden Einfluss hat. Dass öffentliches und nicht privates Datenschutzrecht gilt, ist auch angemessen. Denn es kann nicht sein, dass sich der Staat den ihm auferlegten Grundrechtsbindungen, hier also denen des Grundrechts auf Datenschutz, dadurch entzieht, dass er Aufgaben ausgliedert und privatisiert. Genau dies wäre jedoch die Folge, wenn die Ausgliederung und Privatisierung öffentlicher Aufgaben dazu führen würde, dass sich die datenschutzrechtlichen Pflichten bei der künftigen Aufgabenerledigung in Privatrechtsform nach dem Bundesdatenschutzgesetz richten. Denn obwohl die Umsetzung der europarechtlichen Vorgaben der EG-Datenschutzrichtlinie das nichtöffentliche an das öffentliche Datenschutzrecht annähern wird, bleibt Letzteres in einzelnen Bereichen nach wie vor das strengere Recht.

Was allerdings in Absatz 2 jetzt in der gebotenen Klarheit geregelt ist, wird durch Absatz 4 (bisher: Absatz 3) wieder relativiert. Dort steht nämlich, wie schon bisher, dass als öffentliche Stellen geltende private Einrichtungen, soweit sie als Unternehmen mit eigener Rechtspersönlichkeit am Rechtsverkehr teilnehmen (sog. Wettbewerbsunternehmen), (nur) dem nichtöffentlichen Datenschutzrecht unterliegen. Rein faktisch hat das zur Folge, dass die Mehrzahl der Beteiligungsgesellschaften im Sinne des Absatzes

2 die geringeren Schutzstandards des Dritten Abschnitts des Bundesdatenschutzgesetzes einzuhalten haben. Begründet wird dies damit, dass solche Beteiligungsgesellschaften nicht gegenüber den rein privatrechtlichen Unternehmen, mit denen sie im Wettbewerb stehen, durch strengere Datenschutzerfordernungen benachteiligt werden dürfen. Dies wäre allerdings insoweit keine Besonderheit, als allgemein nach den Grundsätzen des Verwaltungsprivatrechts die Wahrnehmung staatlicher Aufgaben in Privatrechtsform nicht von der Beachtung der Grundrechte entbindet. Auch das Recht auf Datenschutz ist ein Grundrecht, so dass zweifelhaft sein kann, ob die insoweit erfolgte Lockerung der Grundrechtsgebundenheit für Wettbewerbsunternehmen rechtmäßig ist. Beibehalten wurde im Übrigen auch die Besonderheit, dass im Unterschied zu allen anderen Bundesländern solche Wettbewerbsunternehmen in Baden-Württemberg nicht vom Landesbeauftragten für den Datenschutz kontrolliert werden dürfen, sondern der Aufsicht des Innenministeriums unterliegen.

Im neuen Absatz 3 werden die bisher in mehreren Einzelbestimmungen über das Gesetz verstreuten Regelungen über die Anwendbarkeit des Gesetzes auf den Landtag, die Gerichte und den Rechnungshof zusammengefasst. Inhaltlich ändert sich gegenüber der bisherigen Rechtslage dadurch allerdings nichts. Auch damit hat der Gesetzgeber indes die Möglichkeit versäumt, in der Anwendungspraxis bestehende Meinungsverschiedenheiten zu klären. Damals wie heute darf der Landesbeauftragte für den Datenschutz bei den Gerichten die Einhaltung datenschutzrechtlicher Bestimmungen nur prüfen, soweit das Gericht in sog. Verwaltungsangelegenheiten tätig wird. Was unter Verwaltungsangelegenheiten in diesem Sinne gemeint ist und wie weit die Kontrollbefugnis des Landesbeauftragten für den Datenschutz dementsprechend reicht, war zwischen diesem und dem Justizministerium lange Zeit umstritten. In ihrer Entschlie-ßung vom 5./6. Okt. 1998 zu ihrer Prüfungscompetenz bei den Gerichten hatten die Datenschutzbeauftragten des Bundes und der Länder darauf hingewiesen, dass eine Beschränkung ihrer Prüfungscompetenz bei Gerichten einzig und allein den Zweck haben kann, den grundgesetzlich besonders geschützten Bereich der richterlichen Unabhängigkeit von Kontrollen freizuhalten. Während der Landesbeauftragte für den Datenschutz immer davon ausgegangen war, dass die von den Gerichten für ihre automatisierten Verfahren getroffenen technischen und organisatorischen Daten-

sicherheitsmaßnahmen seiner Kontrolle unterliegen und es in seiner Kompetenz liegt zu beurteilen, ob die getroffenen Maßnahmen datenschutzgerecht sind, hatte das Justizministerium den Begriff der Verwaltungsangelegenheiten ohne nähere Begründung sehr eng ausgelegt und darunter nur die Bereiche der Personalverwaltung, Hausverwaltung, des äußeren Geschäftsbetriebs wie z. B. der Materialbeschaffung sowie der Tätigkeit bei Gerichtsverwaltungsakten verstanden. Obwohl mit dem Justizministerium zwischenzeitlich eine weitgehende Übereinstimmung erzielt werden konnte, dass das Bereitstellen automatisierter Datenverarbeitungssysteme oder datenschutzrelevante Vorgaben über die Art und Weise der Datenverarbeitung und der Datensicherung die richterliche Unabhängigkeit nicht betreffen und deshalb der Kontrollkompetenz des Landesbeauftragten für den Datenschutz unterliegen, wäre es angebracht gewesen, in der Regelung über den Geltungsbereich des Landesdatenschutzgesetzes bei Gerichten den Begriff der Verwaltungsangelegenheiten aufzugeben und klar auf die **richterliche Unabhängigkeit** als Grenze abzustellen.

Nach wie vor unregelt bleiben auch die aus datenschutzrechtlicher Sicht problematischen Fälle, in denen öffentliche Stellen private Unternehmen oder Privatpersonen auf vertraglicher Grundlage mit der selbstständigen und eigenverantwortlichen Erledigung von Verwaltungsaufgaben oder Teilen von Verwaltungsaufgaben, einschließlich der dazu notwendigen Datenverarbeitung, betrauen. Auch in diesen Fällen der "Funktionsübertragung" ist es im Ergebnis nicht hinnehmbar, dass sich der Schutz der betroffenen Bürger, soweit es um die Verarbeitung ihrer persönlichen Daten geht, allein aus verwaltungsökonomischen oder haushaltswirtschaftlichen Gründen nicht nach dem öffentlichen Datenschutzrecht richten soll. Zu einer Regelung, wonach private Dritte, die von einer öffentlichen Stelle vertraglich zur Erledigung bestimmter Verwaltungsaufgaben herangezogen werden, vertraglich auch dazu verpflichtet werden, die Bestimmungen des Landesdatenschutzgesetzes zu beachten und sich der Kontrolle durch den Landesbeauftragten für den Datenschutz zu unterwerfen, konnte sich der Gesetzgeber nicht durchringen.

2.2 Die Begriffe des Datenschutzgesetzes - § 3

§ 3 LDSG definiert die wesentlichen Begriffe des Datenschutzrechts. Da manche dieser Begriffe nicht mit der Terminologie der EG-Datenschutzrichtlinie übereinstimmen, wurde das Landesrecht entsprechend angepasst.

Wie schon bisher wird allerdings auch nach neuem Recht zwischen automatisierter und nichtautomatisierter **Datei** unterschieden (§ 3 Abs. 9 LDSG). Inhaltlich bleiben diese Begriffe ebenfalls unverändert. Ob dies mit den europarechtlichen Vorgaben vereinbar ist, darf bezweifelt werden. Denn die Anwendbarkeit vieler datenschutzrechtlicher Bestimmungen hängt davon ab, ob die Datenverarbeitung in oder aus einer Datei oder einer Akte erfolgt. Je weiter der Dateibegriff ausgelegt wird, desto strenger ist das zu beachtende Datenschutzrecht.

Artikel 3 Abs. 1 der EG-Datenschutzrichtlinie kennt lediglich die automatisierte und die nichtautomatisierte (manuelle) **Verarbeitung**. Dabei kommt es für die **automatisierte** Verarbeitung nicht darauf an, ob diese in oder aus einer nach bestimmten Merkmalen auswertbaren Sammlung personenbezogener Daten, also einer Datei, erfolgt. Entgegen dem § 3 Abs. 9 Nr. 1 LDSG spielt deshalb der Dateibegriff im Bereich der automatisierten Verarbeitung keine Rolle.

Die EG-Datenschutzrichtlinie verlangt eine Datei nur im Bereich der **manuellen** Verarbeitung. Dabei fasst sie den Dateibegriff sehr weit, weiter jedenfalls, als der Wortlaut des § 3 Abs. 9 Nr. 2 LDSG dies nahe legt. Denn Artikel 2 Buchst. c der EG-Datenschutzrichtlinie schließt auch Akten, Aktensammlungen sowie ihre Deckblätter ein, soweit diese für eine Benutzung im Hinblick auf die betroffenen Personen organisiert sind, wozu bereits **ein einziges Strukturierungsmerkmal** ausreichen soll (etwa chronologisch abgelegter Schriftverkehr zu einer Person oder alphabetisch nach Namen der Personen geordnete Aktensammlung). Aus dem Dateibegriff sollen allein die "unstrukturierten" Akten herausfallen (Erwägungsgrund 27 der Richtlinie). Nach der Begründung zu Artikel 2 der EG-Datenschutzrichtlinie sind dies (nur) Akten, die nicht für ihre Benutzung im Hinblick auf die betroffenen Personen organisiert sind, deren Struktur also den Zugriff auf und die Suche nach Daten über natürliche Personen nicht erleichtert. Das Landesdatenschutzgesetz ist dagegen enger. Es stellt nicht entscheidend auf die Zugänglichkeit, sondern auf die Auswertbarkeit ab. Denn eine (nichtautomatisierte) Datei soll nur dann vorliegen, wenn es sich um eine

Sammlung personenbezogener Daten handelt, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, ungeordnet und ausgewertet werden kann (ursprünglich dachte man hier an Sammlungen von Karteikarten). Die Anwendung des nationalen Rechts darf aber die Tragweite und die Wirksamkeit des Gemeinschaftsrechts nicht beeinträchtigen. Deshalb muss § 3 Abs. 9 Nr. 2 LDSG in dem Sinne **weit** ausgelegt werden, dass **alle Akten** mit Ausnahme solcher, die völlig unstrukturiert sind, den nichtautomatisierten Dateien zugerechnet werden.

2.3 Die Zulässigkeit der Datenverarbeitung - § 4

Ohne eine gesetzliche Grundlage, die dies ausdrücklich erlaubt, ist die Verarbeitung personenbezogener Daten nur mit Einwilligung der betroffenen Person zulässig. § 4 Abs. 2 LDSG regelt, worüber diese von der verantwortlichen Stelle zu informieren ist, wenn die Einwilligung eingeholt werden soll. Im Vergleich zum bisherigen Recht müssen die Hinweise künftig deutlich ausführlicher erfolgen. Es genügt nun nicht mehr, nur den Verarbeitungszweck darzulegen, also zu sagen, wofür man die Daten braucht. Zu erläutern ist vielmehr auch, wie die Daten verarbeitet werden sollen. Wenn die EG-Datenschutzrichtlinie in diesem Zusammenhang davon spricht, die Einwilligung müsse "in Kenntnis der Sachlage" erfolgen, macht dies deutlicher, wozu diese Mitteilungen dienen sollen. Es geht nämlich darum, der betroffenen Person das Wissen zu verschaffen, das es ihr erlaubt, selbstbestimmt über die Preisgabe und Verwendung ihrer persönlichen Daten zu entscheiden und damit ihr Grundrecht auf Datenschutz wahrzunehmen. Die betroffene Person muss hierzu beispielsweise wissen, in welchem Zusammenhang ihre Daten verwendet werden, wer Zugang zu ihnen hat, welche Maßnahmen zu ihrem Schutz getroffen werden, wann sie wieder gelöscht werden oder an wen die Daten weitergegeben werden. Neu ist auch die Hinweispflicht darauf, dass Daten, die für einen bestimmten Zweck mitgeteilt werden, auf Grund anderer gesetzlicher Bestimmungen unter Umständen ohne weitere Einwilligung für andere Zwecke verwendet werden können. Zu denken ist hier beispielsweise an die in § 15 Abs. 2 und 3 LDSG geregelten Fälle.

Mit Absatz 4 wird der technischen Entwicklung Tribut gezollt. Wer über die technischen Voraussetzungen hierfür verfügt, kann seine Einwilligung

künftig auch in elektronischer Form erteilen. Authentizität und Integrität der Erklärung müssen dabei allerdings gewährleistet sein.

Absatz 6 begründet ein Recht, sich gegen die rechtmäßige Datenverarbeitung zur Wehr zu setzen (sog. Einwendungsrecht). Es kann Fälle geben, in denen der betroffenen Person eine an sich zulässige Datenverarbeitung auf Grund besonderer Umstände gleichwohl nicht zuzumuten ist. Werden solche in der besonderen persönlichen Situation begründeten Interessen vorgebracht und kommt die öffentliche Stelle nach einer Abwägung zu dem Ergebnis, dass diese privaten Interessen das öffentliche Interesse an der Datenverarbeitung überwiegen, dann dürfen die Daten nicht verarbeitet werden. In jedem Fall ist der betroffenen Person, die Einwendungen erhoben hat, das Ergebnis der Abwägung mitzuteilen. Unklar ist noch, in welcher Form dies geschehen muss. Es spricht manches dafür, dass jedenfalls dann, wenn die Abwägung zu Ungunsten der betroffenen Person ausgeht, die Einwendung in Form eines Verwaltungsakts nach § 35 des Landesverwaltungsverfahrensgesetzes zurückzuweisen ist (vgl. etwa BVerwGE 31, 301/306 f.). Hieraus ergeben sich weitere interessante Fragestellungen, wie etwa die, ob ein Widerspruch gegen die ablehnende Entscheidung aufschiebende Wirkung hat und die - wohlgernekt rechtmäßige - Datenverarbeitung deshalb unterbleiben muss, bis die Entscheidung unanfechtbar geworden ist.

Absatz 7 begrenzt automatisierte Einzelentscheidungen. Es geht darum, dass Verwaltungsentscheidungen, die für den Einzelnen mit Nachteilen verbunden sind und die auf Grund eines Persönlichkeitsprofils ergehen, letztlich von einem Menschen getroffen und verantwortet werden müssen. Es darf also nicht so sein, dass solche Entscheidungen ausschließlich automatisiert, von einem Computer getroffen werden. Zulässig ist es dagegen, dass einer Entscheidung automatisiert zu Stande gekommene Vorschläge zu Grunde gelegt werden, da die Entscheidung dann nicht "ausschließlich" auf Grund einer automatisierten Datenverarbeitung ergeht.

2.4 Die Chipkartenregelung - § 5 Abs. 2

Erstmals in das Landesdatenschutzgesetz aufgenommen wurde eine Regelung, die sich mit dem Einsatz mobiler Datenträger, zu denen unter an-

derem Chipkarten zählen, befasst. Inhaltlich wird mit dieser Regelung allerdings nur wenig bestimmt.

Die in Datenschutzkreisen kontrovers diskutierte Frage, ob die Herausgabe dieser Datenträger gesetzlich legitimiert sein muss, wird offen gelassen. Andererseits wird gesehen, dass die Verarbeitung personenbezogener Daten mittels mobiler Datenträger besondere Risiken für das Grundrecht auf Datenschutz birgt. Festgelegt wird deshalb, dass vor dem Einsatz mobiler Datenträger eine Vorabkontrolle durchzuführen ist (§ 12; hierzu später). Im Rahmen dieser Vorabkontrolle sind diese Risiken zu analysieren und festzustellen, ob und gegebenenfalls wie sie vermieden werden können. Die Maßnahmen zur Risikovermeidung sind festzulegen und umzusetzen. Ergibt sich, dass die Risiken zu hoch sind und/oder dass sie nicht beherrschbar sind, kann letztlich nur der Gesetzgeber ihren Einsatz verbindlich festlegen. Denn in wesentlichen, die Grundrechte der Bürger berührenden Fragen ist der Legislative die Entscheidung vorbehalten.

Kommt ein mobiler Datenträger zum Einsatz, sind diejenigen, an die er ausgegeben wird, über ihre in § 5 Abs. 1 LDSG näher bezeichneten Rechte sowie darüber zu informieren, was sie im Falle des Verlusts zu tun haben und womit zu rechnen ist, wenn diese Hinweise nicht beachtet werden. Die verantwortliche Stelle hat auch dafür zu sorgen, dass diese Rechte auf einfache Weise geltend gemacht werden können. So muss es der betroffenen Person ermöglicht werden, sich jederzeit etwa an hierfür bereitgestellten Geräten über die jeweils gespeicherten Daten informieren zu können (§ 5 Abs. 1 Nr. 1). Auch die Berichtigung oder Löschung von Daten auf dem mobilen Datenträger oder deren Sperrung muss ohne unverhältnismäßigen Aufwand möglich sein (§ 5 Abs. 1 Nr. 2). Werden mobile Datenträger ausgegeben, die ohne aktiven Einsatz ihres Inhabers Kommunikationsvorgänge auslösen (z. B. kontaktlose Chipkarten), ist sicherzustellen, dass jeder Kommunikationsvorgang für den Inhaber erkennbar ist. Es darf also vor allem nicht so sein, dass die auf dem Datenträger gespeicherten Informationen abgelesen und verarbeitet werden, ohne dass die betroffene Person dies bemerkt.

2.5 Die Wartung von EDV-Systemen - § 7 Abs. 5

EDV-Systeme müssen gewartet werden. Häufig ziehen die öffentlichen Stellen hierzu externe Unternehmen heran. Im Rahmen der Wartungsarbeiten lässt es sich nicht immer ganz vermeiden, dass der Auftragnehmer personenbezogene Daten zur Kenntnis nehmen kann oder sogar mit diesen Daten arbeiten muss, um Fehler zu beheben. Datenschutzrechtlich handelt es sich bei solchen Wartungsarbeiten nicht um Datenverarbeitung im Auftrag. Denn bei solchen Wartungsvereinbarungen geht es regelmäßig gerade nicht um die Verarbeitung personenbezogener Daten als solche. Diese findet vielmehr nur beiläufig, sozusagen als Begleiterscheinung, statt. Auch hier ist es aber aus Gründen eines wirksamen Datenschutzes erforderlich, einen geeigneten Auftragnehmer auszuwählen. Dieser muss dazu verpflichtet werden, ein Datensicherheitskonzept zu erstellen und vorzulegen, dessen Einhaltung der Auftraggeber zu überwachen hat. Bisher ist man in der Praxis so verfahren, dass § 7 Abs. 2 LDSG in den Fällen der Fremdwartung analog angewandt und mit Wartungsunternehmen entsprechende Verträge abgeschlossen wurden. Diese Praxis wird nun mit § 7 Abs. 5 LDSG auf eine rechtliche Basis gestellt. Auftragsdatenverarbeitung und Wartung der EDV-Anlagen unterliegen jetzt ausdrücklich denselben Voraussetzungen.

2.6 Datenvermeidung und Datensparsamkeit - § 9 Abs. 1

Der neue § 9 Abs. 1 LDSG ist eine der wenigen neuen Regelungen im Landesdatenschutzgesetz, die, wenn sie von der Praxis ernst genommen wird, spürbare Fortschritte beim Datenschutz bringen kann. Dieser Grundsatz der Datenvermeidung und Datensparsamkeit greift nämlich nicht erst ein, wenn die Weichen schon gestellt sind und es nur noch darum gehen kann, Fehler zu reparieren. Künftig müssen die Weichen schon von vornherein richtig gestellt werden. Jede öffentliche Stelle wird sich schon bevor sie Datenverarbeitungsanlagen anschafft und automatisierte Verfahren einrichtet darüber Gedanken machen müssen, in welchem Umfang personenbezogene Daten für eine sachgerechte Aufgabenerfüllung zur Verfügung stehen und wie sie verarbeitet werden müssen. Dieser am Minimalbedarf ausgerichtete Datenumfang bestimmt dann, welche Anlagen und welche Verfahren zu wählen sind.

2.7 Die Datensicherheit („11 Gebote“) - § 9 Abs. 3

Nach § 9 Abs. 3 LDSG sind technisch-organisatorische Maßnahmen zu treffen, um automatisiert verarbeitete personenbezogene Daten zu schützen. Die ehemals in § 9 Abs. 2 LDSG enthaltenen "10 Gebote" wurden um eines (§ 9 Abs. 3 Nr. 10: "Verfügbarkeitskontrolle") ergänzt. Ansonsten blieb alles beim Alten. Damit wurde eine Chance vertan, diesen Bereich des Datenschutzrechts den heutigen Gegebenheiten anzupassen. Der schon seit dem ersten In-Kraft-Treten des Gesetzes im März 1980 im Wesentlichen unveränderte Maßnahmenkatalog entsprach seinerzeit dem damaligen Stand der Technik. Diese war geprägt durch die Großrechner-technologie. Heute sieht die EDV-Landschaft dagegen völlig anders aus. So gut wie jede Behörde ist heute mit vernetzten Einzelplatzcomputern ausgestattet. Die mit der Verarbeitung personenbezogener Daten verbundenen Risiken sind damit heute qualitativ und quantitativ andere als damals. Die Gebote des § 9 Abs. 3 LDSG sind unter heutigen Bedingungen nur noch schwer zu erfüllen. Dies ist in Fachkreisen unbestritten. Wie soll beispielsweise eine Zutrittskontrolle erfolgen, wenn heute in beinahe jedem Büro ein oder mehrere PC stehen? Vorschläge, wie § 9 Abs. 3 LDSG zu modernisieren ist, wurden während des Gesetzgebungsverfahrens gemacht. Sie beruhten im Wesentlichen auf einer vom Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder erarbeiteten Empfehlung. Der Gesetzgeber hat diese Vorschläge bedauerlicherweise nicht berücksichtigt.

2.8 Der behördliche Datenschutzbeauftragte - § 10

Datenschutzbeauftragte bei öffentlichen Stellen waren vor der Gesetzesnovelle eher die Ausnahme. Zwingend vorgeschrieben waren sie allenfalls in einzelnen Bereichen, wie etwa bei (öffentlichen) Krankenhäusern (§ 51 des Landeskrankenhausgesetzes) oder bei Sozialversicherungsträgern (§ 81 Abs. 4 Satz 1 und 4 SGB X). Auch künftig werden öffentliche Stellen nicht gezwungen sein, eigene Datenschutzbeauftragte zu bestellen. Anders als in vielen anderen Ländern und beim Bund stellt § 10 LDSG dies vielmehr ins Belieben jeder öffentlichen Stelle. Begründet wird diese Zurückhaltung damit, man wolle die Selbstverwaltungshoheit der Gemeinden respektieren und die Entscheidung diesen überlassen. Ganz abgesehen davon, dass sich der Gesetzgeber in der Vergangenheit selten geziert hat,

sich eigener Aufgaben zulasten der Gemeinden zu entledigen und dabei wenig Rücksicht auf die kommunale Selbstverwaltung genommen hat, muss man ernsthaft fragen, ob es angesichts der allseits anerkannten Vorteile, die ein örtlicher Datenschutzbeauftragter mit sich bringt, nicht gerade der falsche Punkt war, um Rücksicht zu nehmen. Keinesfalls gerechtfertigt war es aber, mit dem Hinweis auf die kommunale Selbstverwaltung auch die staatlichen Behörden aus der Pflicht zu nehmen.

Der Vorteil eines örtlichen Datenschutzbeauftragten liegt vor allem darin, dass dieser mit dem behördlichen Alltag viel besser vertraut ist, als dies eine zentrale Stelle wie der Landesbeauftragte für den Datenschutz sein kann. Dadurch wird er auch eher in der Lage sein, datenschutzrechtlich relevante Sachverhalte frühzeitig zu erkennen und schnell und effektiv an praxisnahen Lösungen mitzuwirken. Hinzu kommt, dass ein örtlicher Datenschutzbeauftragter bestimmte Aufgaben wahrnehmen kann, wegen der sich die Stelle, für die er tätig wird, ansonsten an den Landesbeauftragten für den Datenschutz wenden müsste. So entfällt die Pflicht, dem Landesbeauftragten für den Datenschutz den Einsatz oder die wesentliche Änderung eines automatisierten Verfahrens zu melden und das Verzeichnis nach § 11 LDSG mitzuteilen (§ 32 LDSG). Ist ein Verfahren der Vorabkontrolle zu unterziehen (§ 12 LDSG), obliegt es dem örtlichen Datenschutzbeauftragten, soweit ein solcher bestellt ist, das Ergebnis der Untersuchung zu prüfen, ansonsten dem Landesbeauftragten für den Datenschutz. Die öffentlichen Stellen sollten deshalb im eigenen Interesse, aber auch im Interesse eines wirkungsvollen Datenschutzes, von dieser neuen Möglichkeit regen Gebrauch machen.

2.9 Das Verzeichnis - § 11

Schon nach dem bisherigen § 10 Abs. 1 LDSG war jede Daten verarbeitende Stelle verpflichtet, ein sog. Verzeichnis zu führen, in dem die eingesetzten Datenverarbeitungsanlagen und die automatisierten Verfahren näher zu beschreiben waren. In der Praxis wurde dieser Pflicht allerdings häufig nicht nachgekommen. Auch die EG-Datenschutzrichtlinie verlangt, dass in einem Verzeichnis über die vorgenommenen Verarbeitungen informiert wird. § 10 Abs. 1 LDSG in seiner neuen Fassung hält deshalb an dieser Verpflichtung fest, verlangt allerdings nicht mehr, dass ein Geräteverzeichnis zu führen ist. Der Katalog der einzutragenden An-

gaben (§ 11 Abs. 2) wurde auf Grund EG-Rechts gegenüber bisher ausgeweitet. Hinzugekommen sind die in den Nummern 1, 6 und 9 genannten Angaben.

Über die konkrete Ausgestaltung eines solchen Verfahrensverzeichnis hat der Landesbeauftragte für den Datenschutz Baden-Württemberg ein Merkblatt herausgegeben. Die verantwortliche Stelle ist verpflichtet, jedem, der dies wünscht, die in § 11 Abs. 2 Nrn. 1 bis 7 LDSG genannten Angaben des Verfahrensverzeichnis "in geeigneter Weise" verfügbar zu machen, ihm also Einblick zu gewähren. Dadurch soll die Datenverarbeitung der öffentlichen Stellen transparent werden. Ist ein örtlicher Datenschutzbeauftragter bestellt, hat dieser das Verfahrensverzeichnis zu führen (§ 10 Abs. 4 Satz 2 Nr. 3 LDSG) und es ist seine Aufgabe, dem interessierten Bürger die Einblicknahme zu ermöglichen.

2.10 Die Vorabkontrolle - § 12

Es gibt Datenverarbeitungen, die auf Grund ihrer Art (z. B. Sensitivität der verarbeiteten Daten; § 12 nennt hier die Daten nach § 33), ihrer Tragweite (betrifft beispielsweise große Teile der Bevölkerung), ihrer Zweckbestimmung (Ausschluss betroffener Personen von Rechten, Vergünstigungen u. Ä.) oder der besonderen Verwendung neuer Technologien (z. B. problematische Erhebungsmethoden wie etwa Videoüberwachung, aber auch der in § 12 Satz 1, 2. Halbsatz genannte Einsatz mobiler Datenträger) besondere Risiken im Hinblick auf das Persönlichkeitsrecht aufweisen. Solche Verarbeitungen sind, bevor sie begonnen werden, darauf zu überprüfen, ob und ggf. unter welchen Voraussetzungen sie mit dem Grundrecht auf Datenschutz zu vereinbaren sind. Die Risikoanalyse und ggf. zu treffende Sicherungsmaßnahmen sind von der verantwortlichen Stelle zu erarbeiten. Ergebnis kann im Einzelfall auch sein, dass die Risiken zu hoch oder nicht beherrschbar sind und die Datenverarbeitung deshalb nicht erfolgen darf. Die verantwortliche Stelle hat das Ergebnis der Untersuchung einschließlich der Begründung dem eigenen Datenschutzbeauftragten oder, wenn ein solcher nicht bestellt ist, dem Landesbeauftragten für den Datenschutz zur Prüfung zuzuleiten.

2.11 Datenerhebung und Videoüberwachung - § 13

§ 13 Abs. 2 LDSG regelt zunächst den Grundsatz, dass personenbezogene Daten beim Betroffenen selbst zu erheben sind. Die bisher in Satz 2 geregelten Hinweispflichten wurden in § 14 Abs. 1 LDSG übernommen. Stattdessen enthält der neue Satz 2 eine Regelung über die Videoüberwachung. Allerdings wird nicht mehr gesagt, als dass, wenn eine Videoüberwachung erfolgen soll, so darauf hingewiesen werden muss, dass hiervon angemessen Kenntnis genommen werden kann. Dies geht nicht weit genug.

Der Bundesgerichtshof hat die Videoüberwachung öffentlicher Räume, der die Betroffenen in der Regel nicht ausweichen können, zu Recht als eine schwerwiegende Beeinträchtigung des allgemeinen Persönlichkeitsrechts bezeichnet (Urteil vom 25.04.95 - VI ZR 272/94). Wird ein öffentlicher Raum per Video überwacht, besteht für jeden, der diesen Raum betritt und unter Umständen sogar betreten muss, quasi ein Zwang zur Angabe personenbezogener Daten. Denn es wird beispielsweise genau registriert, wann sich der Besucher wie lange dort aufgehalten hat, wie er sich verhalten hat, wie er gekleidet war, wer ihn begleitet hat. Nach der Rechtsprechung des Bundesverfassungsgerichts (Volkszählungsurteil vom 15. Dez. 1983, BVerfGE 65, 1 ff.) setzt ein Zwang zur Angabe personenbezogener Daten aber eine **präzise** gesetzliche Regelung voraus. Als solche kann § 13 Abs. 2 Satz 2 LDSG schwerlich bezeichnet werden. Um die mit der Videoüberwachung verbundenen Eingriffe in das Persönlichkeitsrecht zu rechtfertigen, wäre es vielmehr in jedem Fall nötig, gesetzlich festzulegen, für welche Zwecke überwacht werden darf und unter welchen Voraussetzungen Aufnahmen hergestellt werden dürfen und wann diese wieder zu vernichten sind. Neben dem bloßen Hinweis der Betroffenen darauf, dass Videoüberwachung stattfindet, müssten auch Hinweise darauf erfolgen, wozu die Überwachung dient, wer verantwortliche Stelle ist, wie mit eventuellen Aufnahmen weiter verfahren wird, welche Datenschutzrechte dem Betroffenen zustehen und wohin er sich wenden kann, wenn er diese Rechte geltend machen will. Nichts davon steht im Gesetz.

So, wie die Videoüberwachung in § 13 Abs. 2 Satz 2 LDSG derzeit geregelt ist, entspricht sie kaum den verfassungsrechtlichen Vorgaben des Bundesverfassungsgerichts. Hinsichtlich der Videoüberwachung durch den Polizeivollzugsdienst und die Ortspolizeibehörden ist auf die Regelung des § 21 Abs. 3 des Polizeigesetzes hinzuweisen, die im Jahr 2000 eingeführt

wurde. Der Verwaltungsgerichtshof Baden-Württemberg hat in seinem Urteil vom 18. Juli 2003 eine hierauf gestützte Videoüberwachung an Kriminalitätsbrennpunkten in Mannheim im Ergebnis für zulässig erklärt.

Im Übrigen ist § 13 Abs. 4 LDSG "ausgedünnt" worden. Die herausgenommenen Tatbestände wurden aus systematischen Gründen in § 15 Abs. 2 eingefügt.

2.12 Die Unterrichtungspflichten - § 14

Einer der zentralen Punkte, in denen die EG-Datenschutzrichtlinie die Position des Bürgers in datenschutzrechtlicher Hinsicht stärken wollte, ist die Information des Einzelnen über die Verarbeitung seiner Daten durch die jeweilige verantwortliche Stelle. Der Gesetzgeber ist dieser Forderung nachgekommen und hat mit § 14 eigens einen Paragraphen geschaffen, der die Unterrichtung des Betroffenen bei der Erhebung regelt. Inhaltlich ist die Regelung in Teilen allerdings nicht konsequent:

- Nach § 14 Abs. 1 Satz 1 Nr. 2 LDSG ist über die "Empfänger" von Daten nur im Falle der Übermittlung der Daten zu informieren. Da bei einer Datenverarbeitung im Auftrag keine Datenübermittlung an den Auftragnehmer stattfindet (so § 3 Abs. 2 Nr. 4 und Abs. 5 LDSG; die Auftragsdatenverarbeitung gilt als Verarbeitung durch die verantwortliche Stelle selbst), ist demnach auch nicht darüber zu informieren, dass personenbezogene Daten an den Auftragnehmer weitergegeben werden. Die EG-Datenschutzrichtlinie verpflichtet dagegen ganz allgemein dazu, über die Weitergabe von Daten zu informieren, auch wenn der Empfänger ein Auftragsverarbeiter ist. Dass personenbezogene Daten, die von einer öffentlichen Stelle erhoben werden, von dieser zwecks Verarbeitung auch an private Unternehmen weitergegeben werden können, dürfte den wenigsten klar sein. Die Entscheidung, persönliche Verhältnisse zu offenbaren, kann im Einzelfall aber durchaus davon abhängen, dass man weiß, wer hiervon erfährt, insbesondere ob die Daten bei der Behörde bleiben oder nicht. Im Falle der Auftragsdatenverarbeitung wird dem Betroffenen gerade diese Information vorenthalten.
- § 14 Abs. 1 Satz 4 LDSG sieht den Hinweis auf Auskunfts- und Berichtigungsrechte nur vor, wenn die Daten mittels eines Vordrucks erhoben

werden. Die EG-Datenschutzrichtlinie enthält eine solche Einschränkung nicht.

- Nach § 14 Abs. 2 Satz 1 LDSG ist dann, wenn personenbezogene Daten über eine Person nicht offen oder nicht bei dieser selbst, sondern heimlich oder bei Dritten erhoben werden, der Betroffene nur über die beabsichtigte Datenverarbeitung, den Verarbeitungszweck und die Empfänger der Daten zu informieren, wenn die Daten in einer Datei gespeichert werden sollen. Mit anderen Worten: Sollen die Daten in Akten gespeichert werden, sollen keine Informationspflichten bestehen. Eine plausible Erklärung für diese Unterscheidung gibt es nicht.

Eine Benachrichtigungspflicht entfällt, wenn eine der Voraussetzungen des Absatzes 3 vorliegt.

2.13 Datenspeicherung, -veränderung und -nutzung - § 15

§ 15 Abs. 2 LDSG regelt in den Nummern 1 bis 6 Tatbestände, die bisher in § 13 Abs. 4 LDSG geregelt waren. Die Änderung hat allein gesetzgebungstechnische Gründe. Sie vermeidet die unverständlichen Doppelverweisungen, die sich bisher bei der Anwendung des § 13 Abs. 1 und § 15 Abs. 1 LDSG (alt) ergeben hatten.

2.14 Die Wissenschaftsregelungen - § 19 und § 35

Die Bestimmungen des Landesdatenschutzgesetzes, die sich auf die Datenverarbeitung für Zwecke der wissenschaftlichen Forschung beziehen, waren bisher über das Gesetz verteilt. Zudem waren sie lückenhaft. Dies machte es bisher außerordentlich schwer, Fragen nach der Zulässigkeit einer Datenverarbeitung für Forschungszwecke zu beantworten. Die konzentrierte Regelung dieses Bereichs in nunmehr zwei Bestimmungen erleichtert die praktische Arbeit erheblich. Ziel war es dabei auch, die datenschutzrechtlichen Voraussetzungen für Forschungsvorhaben zu erleichtern.

Die §§ 19 und 35 LDSG regeln den Datenschutz in der Forschung aus zwei unterschiedlichen Perspektiven: In § 19 LDSG geht es um die Frage, unter welchen Voraussetzungen öffentliche Stellen dort vorhandene personenbezogene Daten an Forschungseinrichtungen übermitteln dürfen. § 35 LDSG regelt dagegen, unter welchen Voraussetzungen öffentliche

Forschungseinrichtungen personenbezogene Daten erheben dürfen und wie sie im Weiteren mit diesen Daten umzugehen haben.

a. § 19 Abs. 1 LDSG regelt die Datenübermittlung innerhalb des öffentlichen Bereichs, Abs. 2 die Übermittlung an Stellen außerhalb des öffentlichen Bereichs, also an private Forschungseinrichtungen.

aa. Mit § 19 Abs. 1 Satz 1 LDSG wurde im Wesentlichen das übernommen, was bisher in § 13 Abs. 1 und § 12 Abs. 2 Nr. 4 LDSG geregelt war. Kumulativ muss festgestellt werden, dass die Kenntnis der personenbezogenen Daten für das Forschungsvorhaben erforderlich ist (wobei die letzte Alternative, wonach der Forschungszweck ohne den Personenbezug der Daten nicht oder nur mit unverhältnismäßigem Aufwand zu erreichen sein darf, lediglich als Unterfall des Erforderlichkeitsgrundsatzes gesehen werden kann) und das Forschungsinteresse das Interesse des Betroffenen am Ausschluss der Übermittlung **erheblich** überwiegt.

Neu sind die Sätze 2 und 3. In der Regel ist es so, dass es bei Forschungsvorhaben nicht auf die Identität der einbezogenen Personen ankommt, also mit anonymisierten Daten geforscht werden kann. Die Anonymisierung der bei der verantwortlichen Stelle personenbezogen vorliegenden Daten durch die verantwortliche Stelle selbst ist auf Grund des damit verbundenen Arbeitsaufwands in aller Regel nicht zu leisten. In diesen Fällen ist es akzeptabel, wenn die Anonymisierung vor Ort durch Personal der Forschungseinrichtung erfolgt. Allerdings müssen die hierzu eingesetzten Personen in die Organisation der verarbeitenden Stelle eingegliedert, also eine Art "Leiharbeitsverhältnis" begründet werden. Damit erfolgt die Anonymisierung, die selbst eine Form der Datenverarbeitung, nämlich eine Datennutzung, darstellt, faktisch durch die verarbeitende Stelle selbst. Die Verpflichtung nach dem Verpflichtungsgesetz bewirkt, dass sich die mit der Anonymisierung befassten Personen im Falle des Geheimnisbruchs nach § 203 Abs. 2 Satz 1 Nr. 2 StGB strafbar machen.

ab. § 19 Abs. 2 LDSG regelt die Datenübermittlung an private Forschungseinrichtungen. Hier gelten dieselben Grundsätze wie für die Übermittlung an entsprechende öffentliche Einrichtungen. Da

private Einrichtungen grundsätzlich nicht der Geltung des Landesdatenschutzgesetzes, insbesondere dessen § 35, unterliegen, muss die um Übermittlung ersuchte öffentliche Stelle als Voraussetzung für die Zulässigkeit der Übermittlung die empfangende Stelle verpflichten, dass diese die in § 35 Abs. 2 und 3 LDSG genannten Bedingungen beachtet.

- b. Die wesentliche Neuerung in § 35 LDSG ist, dass es jetzt eine ausdrückliche Datenerhebungsbefugnis für wissenschaftliche Forschungsvorhaben gibt (§ 35 Abs. 1 Satz 1 und 2 LDSG). Der bisherige Absatz 2 ist inhaltlich in § 19 Abs. 2 LDSG übernommen worden.

Exkurs: Mit der Änderung des Landesdatenschutzgesetzes durch das Gesetz vom 23. Mai 2000 wurde auch das Landeskrankenhausgesetz (LKHG) insoweit geändert, als Krankenhäuser nun nach § 46 Abs. 1 Satz 1 Nr. 2a LKHG befugt sind, erforderlichenfalls Patientendaten zur Durchführung eigener medizinischer Forschungsvorhaben zu übermitteln. Damit ist vor allem das Problem beseitigt, dass in den Fällen, in denen das Krankenhaus für Forschungszwecke feststellen muss, ob ein ehemaliger Patient noch lebt und sich deshalb an die Meldebehörde wendet, um von dort das Sterbedatum zu erfahren, mit dieser Anfrage der Meldebehörde automatisch mitteilt, die betreffende Person sei im Krankenhaus behandelt worden. Schon diese Information fällt unter die ärztliche Schweigepflicht. Solche Anfragen bedürfen deshalb einer gesetzlichen Ermächtigung, es sei denn, der Patient hat insoweit von der Schweigepflicht entbunden. Zwar ist es so, dass nach § 43 Abs. 3 LKHG die bereichsspezifischen Regelungen des Landeskrankenhausgesetzes gerade nicht für die Verarbeitung von Patientendaten für Zwecke der wissenschaftlichen Forschung und Lehre gelten sollen. Das Landeskrankenhausgesetz lässt damit den gesamten Bereich der wissenschaftlichen Forschung im und durch das Krankenhaus ungeregelt. Damit bleibt es für öffentliche Krankenhäuser grundsätzlich bei der Anwendbarkeit der Forschungsklauseln des Landesdatenschutzgesetzes, für private Krankenhäuser bei denen des Bundesdatenschutzgesetzes. Gleichwohl berechtigt § 19 LDSG das (öffentliche) Krankenhaus nicht, Patientendaten zu übermitteln. Denn die ärztliche Schweigepflicht steht nach § 2 Abs. 5 LDSG selbstständig neben den allgemeinen Datenschutzbestimmungen. Als allgemeines Gesetz ist das

Landesdatenschutzgesetz, im Gegensatz zum speziellen Landeskrankenhausesgesetz, nicht geeignet, die Offenbarung von Patientengeheimnissen zu rechtfertigen. § 46 Abs. 1 Satz 1 Nr. 2a LKHG, der im Hinblick auf § 43 Abs. 3 LKHG einen systematischen Bruch darstellt, gibt dagegen einen spezifischen Rechtfertigungsgrund.

2.15 Datenübermittlung ins Ausland - § 20

Die Regelung über die Datenübermittlung ins Ausland wurde vollständig überarbeitet und neu gefasst. Die Übermittlung personenbezogener Daten in Mitgliedstaaten der Europäischen Union und die Übermittlung an Organe und Einrichtungen der Europäischen Gemeinschaften ist nun der Übermittlung an Stellen im Geltungsbereich des Grundgesetzes gleichgestellt (Absatz 1). Für die Übermittlung in andere Staaten oder an andere über- oder zwischenstaatliche Einrichtungen gilt ein nicht einfach zu erfassendes Regelwerk. In Absatz 3 werden Sachverhalte angegeben, bei deren Vorliegen eine Übermittlung in solche Staaten oder an solche Einrichtungen unzulässig ist. Neben dem Verstoß gegen ein deutsches Gesetz geht es dabei vor allem um die Fälle, in denen in dem Drittland oder bei der zwischenstaatlichen Stelle kein angemessenes Datenschutzniveau gewährleistet ist. Dies muss im Einzelfall im Wege der Abwägung ermittelt werden. Selbst wenn festgestellt wird, dass ein solches angemessenes Schutzniveau nicht besteht, kann eine Übermittlung unter den in den Absätzen 4 und 5 genannten Voraussetzungen zulässig sein. Nach Absatz 5 reicht die vertragliche Garantie des Empfängers, das Persönlichkeitsrecht zu schützen, aus, um Daten auch in Staaten zu übermitteln, die ansonsten kein angemessenes Datenschutzniveau gewährleisten.

Gemäß Artikel 25 Abs. 6 der EG-Datenschutzrichtlinie kann die Kommission mit Unterstützung des nach Artikel 31 eingesetzten Ausschusses feststellen, dass ein Drittland ein angemessenes Schutzniveau gewährleistet. Diese Feststellung ermöglicht die Übermittlung personenbezogener Daten durch die Mitgliedstaaten, ohne dass zusätzlich Garantien erforderlich sind. Die Kommission trifft ihre Feststellungen auf der Grundlage von Empfehlungen einer "Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten" (Artikel 29 und 30 der EG-Datenschutzrichtlinie, sog. Artikel 29 - Datenschutzgruppe).

2.16 Das Auskunftsrecht - § 21

Geringfügig erweitert wurden die Gesichtspunkte, über die die verantwortliche Stelle der betroffenen Person Auskunft zu geben hat. So erstreckt sich die Auskunftspflicht auch auf den Verarbeitungszweck und, wenn einzelne persönliche Aspekte der betroffenen Person automatisiert bewertet werden, auch darauf, wie dieses automatisierte Verfahren strukturiert ist und welche Kriterien der Entscheidung - über die Ergebnisse einer automatisierten Auswertung hinaus - noch zu Grunde gelegt worden sind (Verbot der automatisierten Einzelentscheidung, § 4 Abs. 7 LDSG).

Absatz 3 räumt der betroffenen Person jetzt grundsätzlich ein Akteneinsichtsrecht ein. Bisher war die Akteneinsicht eine Form der Auskunftserteilung unter anderen. Sie zu gewähren, lag im Ermessen der verantwortlichen Stelle. Dieses Ermessen wird jetzt in eine Verpflichtung umgewandelt. Liegen die Voraussetzungen für eine Versagung nicht vor, muss Akteneinsicht gewährt werden. Dieses Recht geht weiter als das verwaltungsverfahrensrechtliche Akteneinsichtsrecht, das als unbedingtes Recht nur bis zum Abschluss des Verwaltungsverfahrens gilt. Danach besteht nur noch ein Anspruch, ermessensfehlerfrei über das Akteneinsichtsbegehren zu entscheiden.

2.17 Die Berichtigung unrichtiger Daten, Löschung und Sperrung - §§ 22 bis 24

Schon bisher war in § 18 Abs. 2 LDSG die Pflicht der verantwortlichen Stelle geregelt, dann, wenn unrichtige personenbezogene Daten nachträglich zu berichtigen waren, dies auch denjenigen mitzuteilen, denen sie die Daten zuvor übermittelt hatte. § 22 Abs. 2 LDSG ändert dies nur redaktionell. Den Vorgaben der EG-Datenschutzrichtlinie wird dies nicht gerecht. Nach deren Artikel 12 Buchstabe c haben die Mitgliedstaaten den Betroffenen zu garantieren, dass Dritte, die in den Besitz unrichtiger Daten gelangt sind, von der verantwortlichen Stelle über jede Berichtigung informiert werden. Eine Ausnahme hiervon ist nur zulässig, wenn diese Information unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden ist. Nach EG-Recht darf es also für die Frage, ob diejenigen, denen die verantwortliche Stelle unrichtige Daten mitgeteilt hat, über die Berichtigung zu informieren sind, nicht, wie dies in § 22 Abs. 2 LDSG geregelt ist,

auf die subjektive Einschätzung der verantwortlichen Stelle ankommen, ob eine solche Information erforderlich erscheint oder nicht.

Indem § 23 Abs. 5 und § 24 Abs. 5 LDSG auf § 22 Abs. 2 LDSG verweisen, gilt das oben Gesagte für die Löschung und Sperrung von Daten entsprechend.

2.18 Die Schadensersatzregelung - § 25

Der datenschutzrechtliche Schadensersatzanspruch ist gegenüber der bisherigen Regelung deutlich erweitert worden. Bisher konnte ein solcher Anspruch nur dann entstehen, wenn Daten im Laufe einer automatisierten Verarbeitung unrichtig wurden oder wenn Dritte eine automatisierte Sicherungseinrichtung überwinden und sich Daten beschaffen konnten. Dieser Technikbezug wird aufgegeben. § 25 Abs. 1 LDSG räumt einen Ersatzanspruch immer dann ein, wenn der betroffenen Person dadurch ein Schaden entstanden ist, dass eine öffentliche Stelle personenbezogene Daten in oder aus einer Datei unzulässig oder unrichtig verarbeitet. Das Verschulden der öffentlichen Stelle wird dabei widerlegbar vermutet.

2.19 Der Landesbeauftragte für den Datenschutz - §§ 26 bis 32

Nach neuem Recht kann künftig auch zum Landesbeauftragten für den Datenschutz bestellt werden, wer für eine andere Laufbahn des höheren Dienstes als für das Richteramt oder den höheren Verwaltungsdienst befähigt ist (§ 26 Abs. 1 Satz 1 LDSG). Damit soll auch Bewerberinnen besonderer Fachrichtungen der Zugang zu dem Amt eröffnet werden. Neu ist auch die zeitliche Begrenzung der Amtsinhaberschaft auf maximal 16 Jahre (§ 26 Abs. 1 Satz 2 LDSG).

Erweitert werden die Kontrollbefugnisse des Landesbeauftragten für den Datenschutz in § 28 LDSG. Weggefallen ist die anlassabhängige Kontrolle von Akten. Allerdings werden sich die praktischen Auswirkungen dieser Erleichterung in Grenzen halten. Denn bei richtlinienkonformer Auslegung des Begriffs der nichtautomatisierten Datei (§ 3 Abs. 9 Nr. 2 LDSG; siehe oben) käme ohnehin einem Großteil der Akten Dateiqualität zu. Für die Kontrolle von Dateien bedurfte es aber bereits bisher keines konkreten

Anhaltspunkts für eine Datenschutzverletzung. Weggefallen ist auch die Möglichkeit für die betroffene Person, der Verarbeitung ihrer dem Arztgeheimnis unterliegenden oder ihrer Personaldaten durch den Landesbeauftragten für den Datenschutz und seine Mitarbeiter anlässlich einer Kontrolle einer öffentlichen Stelle zu widersprechen.

Völlig neu gestaltet wird der bisherige § 28 LDSG (jetzt § 32). Nach Absatz 1 haben die öffentlichen Stellen dem Landesbeauftragten für den Datenschutz den Einsatz und die wesentliche Veränderung eines automatisierten Verfahrens zu melden. Die Meldepflicht entfällt, wenn die öffentliche Stelle einen eigenen Datenschutzbeauftragten bestellt hat. Sie entfällt ebenfalls, soweit es um automatisierte Register geht, die ausschließlich zur Information der Öffentlichkeit bestimmt sind, und bei Verfahren, die allgemeinen Verwaltungszwecken dienen. Das Landesamt für Verfassungsschutz muss generell seine Verfahren nicht melden. Neben dieser Meldung sind dem Landesbeauftragten für den Datenschutz die Angaben aus dem Verzeichnisse nach § 11 Abs. 2 LDSG mitzuteilen. Offen bleibt im Gesetz dagegen, wie der Landesbeauftragte für den Datenschutz mit den Meldungen verfahren soll. Die bisher bestehende Pflicht, ein Datenschutzregister zu führen, wurde abgeschafft. Die Meldungen müssen auch nicht mehr für Auskünfte an Bürger bereitgehalten werden. Diese Verpflichtung obliegt nach § 11 Abs. 4 Satz 1 LDSG der verantwortlichen Stelle vor Ort.

2.20 Die personenbezogenen Daten 'besonderer Art' - § 33

Artikel 8 der EG-Datenschutzrichtlinie bestimmt eine besondere Kategorie personenbezogener Daten (auch 'sensitive' Daten genannt), deren Verarbeitung grundsätzlich zu untersagen ist. Es geht dabei um Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie um Daten über Gesundheit oder Sexualleben. Ausnahmsweise dürfen solche Daten unter den in Artikel 8 der Richtlinie genannten Voraussetzungen verarbeitet werden. § 33 LDSG setzt diese europarechtlichen Vorgaben um.

Absatz 1 der Vorschrift gibt den engen Rahmen vor, in dem solche sensiblen Daten zulässigerweise verarbeitet werden dürfen. Von der Einwilligung und dem Schutz lebenswichtiger Interessen der betroffenen Person selbst oder eines Dritten abgesehen, ist eine "besondere" Rechtsvorschrift erforderlich, die die Verarbeitung dieser Daten vorsehen muss. Die Bestimmungen des Landesdatenschutzgesetzes sind demnach nicht geeignet, eine Verarbeitung solcher sensiblen Daten zu rechtfertigen.

Die Absätze 2 und 3 bestimmen, wo das Verarbeitungsverbot nicht gilt. Zulässig ist eine Verarbeitung sensibler Daten danach in bestimmten Bereichen (wissenschaftliche Forschung, Personalwesen, Gefahrenabwehr, Strafverfolgung, Sicherheitsüberprüfung) oder durch bestimmte Stellen (Landesamt für Verfassungsschutz, Finanzverwaltung, öffentlich-rechtliche Religionsgemeinschaften, wobei Letztere insoweit nur Daten über religiöse und weltanschauliche Überzeugungen verarbeiten dürfen).

2.21 Der Personaldatenschutz - § 36

§ 36 LDSG, der den bisherigen § 2 Abs. 2 LDSG ablöst, regelt das für Arbeiter und Angestellte im öffentlichen Dienst geltende Datenschutzrecht entsprechend dem für Beamte geltenden Datenschutzrecht. Absatz 1 betrifft die Verarbeitung von Personaldaten außerhalb von Personalakten, Absatz 2 die Verarbeitung von Personalaktendaten. In Absatz 1 wird - wie etwa auch in § 113 Abs. 1 Satz 3 und Abs. 4 Satz 1 des Landesbeamtengesetzes - die Zweckbindung hinsichtlich des Verarbeitens personenbezogener Daten von Beschäftigten besonders geregelt. Der Begriff der Personalakten(daten) bezieht sich dabei auf die Verarbeitung von Daten in Papierakten sowie in automatisierten Verfahren. Absatz 3 trifft besondere Regelungen zum Umgang mit Bewerberdaten.

3. Ergänzende Informationen

3.1 Aktuelle Fassung des Landesdatenschutzgesetzes

Die aktuelle Textfassung finden Sie unter
www.baden-wuerttemberg.datenschutz.de/recht/ldsg/default.htm

3.2 Virtuelles Datenschutzbüro

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

www.datenschutz.de