Verwaltungsvorschriften zum Niedersächsischen Datenschutzgesetz

Gem. RdErl. d. MI, d. StK u. d. übr. Min. v. 26.6.2002 - 44.22-05419/2 -

Vom 26. Juni 2002 (Nds. MBl. S. 640)

- VORIS 20600 -

Bezug:

Gem. RdErl. v. 23.6.1994 (Nds. MBI. S. 1147), geändert durch Gem. RdErl. v. 11.5.1998 (Nds. MBI. S. 920)
- VORIS 20600 02 00 00 001 -

Zu § 2 (Anwendungsbereich)

1.1 Neben den öffentlichen Stellen im engeren Sinne findet das NDSG auch Anwendung auf Vereinigungen des Landes, der Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, die privatrechtlich (z.B. als eingetragener Verein oder GmbH) organisiert sind (vgl. & 2 Abs. 2 des Bundesdatenschutzgesetzes FBDSGI). Um eine Vereinigung in diesem Sinne handelt es sich allerdings nur, wenn sie von mehreren der in & 2 Abs. 1 Satz 1 Nrn. 1 bis 3 genannten Stellen gebildet wird. Eine nur vom Land oder einer Gemeinde gegründete Gesellschaft unterliegt nicht dem NDSG, sondern den Bestimmungen des BDSG, die für nicht öffentliche Stellen gelten. Dies gilt auch für Vereinigungen, an denen sowohl öffentliche Stellen als auch nicht öffentliche Stellen (natürliche Personen oder juristische Personen des privaten Rechts) beteiligt sind.

1.2 Die in § 2 Abs. 3 genannten wirtschaftlichen Unternehmen und sonstigen Einrichtungen, die überwiegend wirtschaftliche Aufgaben wahrnehmen bzw. am Wettbewerb teilnehmen, werden hinsichtlich der materiellen Datenschutzregelungen weitgehend wie private Stellen behandelt und unterliegen, soweit personenbezogene Daten in Ausübung ihrer wirtschaftlichen Tätigkeit verarbeitet werden, den Vorschriften des BDSG für nicht öffentliche Stellen. Hierzu zählen die Eigenbetriebe gemäß § 108 Abs. 2 Nr. 1 NGO (z.B. Verkehrs- und Versorgungsbetriebe) und die öffentlichen Einrichtungen, die entsprechend den Vorschriften über die Eigenbetriebe geführt werden. Krankenhäuser in öffentlich-rechtlicher Trägerschaft gehören unabhängig von ihrer Zuordnung nach § 116a Abs. 2 Satz 2 NGO zu den Einrichtungen i.S. des § 2 Abs. 3 Satz 1 Nr. 1, die am Wettbewerb teilnehmen. Dies gilt jedoch nicht, soweit Krankenhäuser hoheitliche Aufgaben (z.B. im Rahmen von Zwangseinweisungen) wahrnehmen.

Soweit Hochschulkliniken der Patientenversorgung dienen, gehören sie zu den Einrichtungen, die am Wettbewerb teilnehmen. Gleiches gilt für die Erbringung von Leistungen gewerblicher Art (z.B. Laboruntersuchungen und gutachterliche Stellungnahmen). Hinsichtlich der übrigen von ihnen wahrzunehmenden Aufgaben, z.B. Lehre und Forschung, unterliegen sie uneingeschränkt den Regelungen des NDSG.

Für die Verarbeitung personenbezogener Daten der Beschäftigten dieser Stellen ist ebenso wie bei den öffentlichen Stellen nach § 2 Abs. 1 Satz 1 das NDSG i.V.m. den bereichsspezifischen datenschutzrechtlichen Regelungen in den §§ 101 bis 101h i.V.m. § 261 Abs. 1 Nr. 2 NBG anwendbar, da sie nicht unmittelbar wirtschaftlichen Zwecken dient und die Daten damit nicht in Ausübung wirtschaftlicher Tätigkeit verarbeitet werden. Auch die Aufsichtsbefugnisse der oder des Landesbeauftragten für den Datenschutz ergeben sich uneingeschränkt aus dem NDSG.

1.3 Für öffentlich-rechtliche Kreditinstitute und Versicherungsanstalten sowie deren Vereinigungen enthält § 2 Abs. 4 eine spezielle Regelung. Auf diese Stellen findet abweichend von § 2 Abs. 3 nur § 24 i.d.F. vom 17.6.1993 als bereichsspezifische Regelung für die Datenverarbeitung personenbezogener Daten bei Dienst- und Arbeitsverhältnissen Anwendung.

1.4 § 2 Abs. 7 enthält eine klarstellende Regelung für das Verhältnis des NDSG zum Nds. VwVfG. Die in § 1 Abs. 1 Satz 1 Nds. VwVfG i.V.m. § 24 VwVfG enthaltenen Regelungen über Art und Umfang der Ermittlungen und die Regelungen in § 1 Abs. 1 Satz 1 Nds. VwVfG i.V.m. § 26 VwVfG über die zugelassenen Beweismittel (insbesondere Einholung von Auskünften und Anhörung von Beteiligten, Zeugen sowie Beiziehung von Urkunden und Akten) werden durch die Regelungen des NDSG verdrängt, soweit personenbezogene Daten erhoben werden sollen. Auch eine Übermittlung personenbezogener Daten im Wege der Amtshilfe ist nur im Rahmen der einschränkenden Bestimmungen des NDSG, insbesondere über die Zweckbindung (§ 11 Abs. 1 i.V.m. § 10 Abs. 2), zulässig (vgl. § 5 Abs. 2 Nr. 1 VwVfG).

Die in § 29 VwVfG geregelte Akteneinsicht der Verfahrensbeteiligten besteht dagegen neben dem Recht auf Auskunft und Einsicht in Akten nach § 16. Dies gilt auch, soweit Verfahrensbeteiligte im Rahmen einer Akteneinsicht nach § 29 VwVfG personenbezogene Daten Dritter zur Kenntnis erhalten (vgl. § 13 Abs. 1 Satz 1 Nr. 2). Bereichsspezifische und da mit dem NDSG vorgehende Regelungen sind insbesondere in den Bestimmungen im VwVfG über Planfeststellungsverfahren (Teil V) enthalten, soweit diese Regelungen die Verarbeitung personenbezogener Daten zwingend voraussetzen, z.B. durch die in § 74 Abs. 4 VwVfG vorgeschriebene Zustellung und öffentliche Auslegung des Planfeststellungsbeschlusses. Einschränkungen für die Zulässigkeit der damit verbundenen Datenübermittlung ergeben sich allerdings im Einzelfall aus dem Verhältnismäßigkeitsgrundsatz (vgl. Beschluss des Bundesverfassungsgerichts vom 24.7.1990 - BvR 1244/87 -, DVBI. S. 1041). Auch unter Berücksichtigung des in Massenverfahren besonders gewichtigen Gesichtspunktes der Verwaltungspraktikabilität muss danach geprüft werden, inwieweit eine ordnungsgemäße Begründung des Planfeststellungsbeschlusses notwendig voraussetzt, dass die inhaltliche Auseinandersetzung mit den geltend gemachten Einwendungen personenbezogen erfolgt und mit der Begründung veröffentlicht wird.

Zu § 3 (Begriffsbestimmungen)

2.1 Das NDSG geht von einem umfassenden Begriff der Datenverarbeitung aus. § 3 Abs. 2 umfasst daher auch jede aktenmäßige Verarbeitungsform.

Bei der Weitergabe von Daten innerhalb einer Behörde im organisatorischen Sinne handelt es sich nicht um ein Übermitteln, das nach § 3 Abs. 2 Satz 2 Nr. 4 eine Bekanntgabe an Dritte voraussetzt, sondern um ein Nutzen personenbezogener Daten. Die Zulässigkeit der behördeninternen Datenweitergabe richtet sich nach § 11 Abs. 4.

2.2 Die Pflichten des NDSG treffen die für die Datenverarbeitung verantwortliche Stelle. Da im öffentlichen Bereich die Daten verarbeitende Stelle in der Regel auch die für die Datenverarbeitung verantwortliche Stelle ist, hat der Gesetzgeber von einer Anpassung an den Wortlaut der EG-Datenschutzrichtlinie abgesehen. Die Daten verarbeitende Stelle bleibt auch bei der Beauftragung anderer Behörden und externer Dienstleister für die Einhaltung der datenschutzrechtlichen Bestimmungen während der von ihr veranlassten Verarbeitungen verantwortlich.

2.3 Das novellierte NDSG verzichtet auf die Verwendung des Dateibegriffs. Sowohl die Begriffsbestimmung der automatisierten wie der nicht automatisierten Datei entfällt. An die Stelle der Dateibeschreibung ist die Verfahrensbeschreibung getreten. Da automatisierte Dateien nur mit Hilfe von automatisierten Verarbeitungen erzeugt oder ausgewertet werden können, sind sie stets als Bestandteil einer automatisierten Verarbeitung anzusehen. Soweit in bereichsspezifischen Regelungen der Begriff der automatisierten Datei verwendet wird, finden demzufolge darauf ergänzend die Bestimmungen für die automatisierte Verarbeitung Anwendung.

Zu § 4 (Zulässigkeit der Datenverarbeitung)

3.1 Soweit die Datenverarbeitung auf eine Rechtsgrundlage gestützt werden kann, widerspricht es den Zielen des NDSG, wenn von Betroffenen eine Einwilligungserklärung eingeholt wird.

3.2. Eine wirksame Einwilligung setzt voraus, dass insbesondere der Zweck der Verarbeitung und beabsichtigten Übermittlungen Bestandteil der Einwilligungserklärung sind. Der Umfang der Ermächtigung zur Datenverarbeitung ergibt sich in diesen Fällen grundsätzlich aus den Festlegungen in der Einwilligungserklärung. Ausnahmen hiervon sind lediglich die aus überwiegendem Allgemeininteresse vorgesehenen speziellen Vorschriften über die zweckdurchbrechende Verarbeitung erhobener oder gespeicherter Daten (§ 10).

Die Verarbeitung personenbezogener Daten nach § 4 Abs. 2 Satz 2 setzt eine bereichsspezifische gesetzliche Ermächtigung oder eine Einwilligung voraus, in der ausdrücklich die zu verarbeitenden Kategorien von Daten nach § 4 Abs. 2 Satz 2 genannt werden.

Zu § 6 (Verarbeitung personenbezogener Daten im Auftrag)

4.1 Soweit personenbezogene Daten im Rahmen der Wartung oder Fernwartung von Datenverarbeitungssystemen zwingend genutzt werden müssen, ist dies als Datenverarbeitung im Auftrag i.S. des § 6 zulässig. Ob weitergehende Schutzvorschriften (z.B. § 203 des Strafgesetzbuches FStGBl) berührt sind, ist gesondert zu prüfen.

4.2 Lässt eine öffentliche Stelle des Landes personenbezogene Daten im Auftrag von einer Stelle außerhalb des Landes Niedersachsen verarbeiten, so hat der Auftraggeber die zuständige Datenschutzkontrollbehörde zu unterrichten. Handelt es sich bei dem Auftragnehmer um eine öffentliche Stelle eines anderen Landes oder des Bundes, so ist zuständige Datenschutzkontrollbehörde die oder der jeweilige Landesdatenschutzbeauftragte bzw. die oder der Bundesbeauftragte für den Datenschutz. Handelt es sich bei dem Auftragnehmer um eine nicht öffentliche Stelle, ist die nach § 38 BDSG zuständige Aufsichtsbehörde zu unterrichten.

Im Rahmen der vertraglichen Verpflichtung nicht öffentlicher Stellen als Auftragnehmer, jederzeitige vom Auftraggeber veranlasste Kontrollen zu ermöglichen, ist auch das Prüfungsrecht der oder des Landesbeauftragten für den Datenschutz zu gewährleisten. In jedem Fall haben sich die Auftraggeber von der Beachtung der Regelungen des § 7 und der Einhaltung der erteilten Weisungen zu vergewissern.

Zu § 6a (Mobile personenbezogene Speicher- und Verarbeitungsmedien)

5.1 Mit dem Begriff "mobile personenbezogene Speicher und Verarbeitungsmedien" werden nach dem heutigen Stand der Technik vor allem Chipkarten erfasst. Die Vorschrift erfasst nur solche Speicher- und Verarbeitungsmedien, auf denen personenbezogene Daten der Karteninhaberin oder des Karteninhabers verarbeitet werden; die mobilen personenbezogenen Speicher- und Verarbeitungsmedien müssen von einer öffentliche Daten verarbeitenden Stelle ausgegeben worden sein. Nicht erfasst werden tragbare Computer (z.B. Laptop, Palmtop, WAP), die an Mitarbeiterinnen oder Mitarbeiter zur Aufgabenerfüllung herausgegeben werden.

5.2 Der Pflicht, den Betroffenen die Kenntnisnahme der auf dem Medium gespeicherten Daten zu ermöglichen, wird auch genügt, wenn die für Zwecke der Verarbeitung aufgestellten Endgeräte zusätzlich eine Funktion bieten, die es der Karteninhaberin oder dem Karteninhaber ermöglicht, die auf der Karte gespeicherten personenbezogenen Daten einzusehen. Soweit die weitergehenden Rechte nach §§ 16 und 17 nicht als Funktion zur Verfügung stehen, sind Hinweise zu geben, gegenüber welcher Stelle die Betroffenen ihre Rechte geltend machen können.

5.3 Um zu verhindern, dass ein Datenaustausch ohne Kenntnis der Karteninhaberin oder des Karteninhabers erfolgt (z.B. bei berührungslosen Chipkarten), verpflichtet Absatz 3 die beteiligten Stellen, die Tatsache der Kommunikation für die betroffene Person eindeutig erkennbar zu machen (z.B. durch akustische Signale).

Zu § 7 (Technische und organisatorische Maßnahmen)

6.1 Unabhängig davon, ob personenbezogene Daten in Akten oder automatisiert verarbeitet werden, haben die öffentlichen Stellen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um eine datenschntzgerechte Verarbeitung der Daten sicherzustellen.

Die Datensicherung kann dann als wirksam angesehen werden, wenn die getroffenen technischen und organisatorischen Maßnahmen in ihrer Gesamtheit einen hinreichenden Schutz der Daten vor Missbrauch bieten.

6.2 Von einer Novellierung der nach Absatz 2 zu treffenden Maßnahmen, um diese den veränderten technischen Begrifflichkeiten anzupassen, hat der Gesetzgeber Abstand genommen, weil eine entsprechende Neuregelung auch auf Bundesebene erst im Rahmen einer vom BMI beabsichtigten grundlegenden Novellierung des BDSG erfolgen soll und für die Zwischenzeit keine neuen Begriffe eingeführt werden sollten, die bereits in Kürze wieder geändert werden müssten. Neu ist die Regelung nach Nr. 8, mit der die Daten verarbeitende Stelle einer Forderung der EG-Datenschutzrichtlinie entsprechend nunmehr auch gesetzlich verpflichtet wird, die Verfügbarkeit der personenbezogenen Daten zu gewährleisten.

Das Datensicherungskonzept ist regelmäßig zu überprüfen und dem Stand der Technik anzupassen. Dem jeweiligen Stand der Technik entsprechen fortschrittliche Maßnahmen, die die praktische Eignung zur Sicherstellung einer datenschutzgerechten Verarbeitung personenbezogener Daten gesichert erscheinen lassen, insbesondere mit Erfolg erprobt worden sind. Bei der Auswahl technischer Maßnahmen sollten grundsätzlich sicherheitsüberprüfte und zertifizierte Produkte bevorzugt werden. Einen aktuellen Nachweis über zertifizierte Produkte führt das Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 183, 53133 Bonn.

6.3 Verfahren, die wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien besondere Risiken in sich tragen, sind vor ihrer Einführung einer Vorabprüfung (Technikfolgenabschätzung) durch die Beauftragte oder den Beauftragten für den Datenschutz zu unterziehen, um festzustellen, ob die mit der automatisierten Verarbeitung verbundenen Risiken für die Rechte der Betroffenen durch technische und organisatorische Maßnahmen wirksam beherrscht werden können. Personenbezogene Daten, deren automatisierte Verarbeitung besondere Risiken für die Rechte der Betroffenen mit sich bringen, sind solche, deren Missbrauch oder Verlust Existenz, Leben oder Freiheit der Betroffenen gefährden oder sie in ihrer gesellschaftlichen Stellung erheblich beeinträchtigen würden. Als neu sind Technologien einzustufen, die erstmals im Anwendungsbereich des NDSG zum Einsatz kommen und bei denen noch nicht abschätzbar ist, ob die mit der Verarbeitung verbundenen Risiken für die Rechte der Betroffenen mit Maßnahmen nach § 7 Abs. 2 beherrscht werden können.

Die Ergebnisse der Technikfolgenabschätzung sind schriftlich zu dokumentieren. Dabei sind den denkbaren Gefährdungen die möglichen Sicherungs- und Vorbeugungsmaßnahmen gegenüberzustellen und verbleibende Gefahren für die Rechte der Betroffenen darzustellen und zu bewerten. Verfahrensalternativen zur angestrebten Lösung sind aufzuzeigen.

6.4 Mit § 7 Abs. 4 wird der Grundsatz der Datensparsamkeit und -vermeidung eingeführt. Die Daten verarbeitenden Stellen werden verpflichtet, bei der Auswahl und dem Einsatz von automatisierten Verfahren das Ziel zu beachten, keine oder so wenig wie möglich personenbezogene Daten zu verarbeiten. Danach ist bereits im Vorfeld bei Entwicklung und Auswahl von Datenverarbeitungssystemen darauf hinzuwirken, dass keine oder möglichst wenig personenbezogene Daten verarbeitet werden müssen. Es gibt damit ein übergreifendes Gestaltungsprinzip vor, das aus dem Tele- und Medienrecht übernommen worden ist und das Entstehen von Daten mit Personenbezug oder Personenbeziehbarkeit von vornherein ausschließen oder auf ein Minimum beschränken will. Dieses Prinzip ist Bestandteil eines neuen

Ansatzes, der über einen Systemdatenschutz eine Reduzierung der Risiken für die informationelle Selbstbestimmung erreichen will. Auswirkungen hat es z.B. hinsichtlich der Verarbeitung von personenbezogenen Daten der Beschäftigten, soweit diese benötigt werden für Zwecke der Dokumentation der Kommunikation (E-Mail-Adresse), der Protokollierung von Intra- und Internetnutzung sowie zur Überwachung der Nutzung der Datenverarbeitungsanlagen. Soweit zur Vermeidung von Missbräuchen oder zur Abwehr unzulässiger Zugriffe und Nutzungen eine Protokollierung notwendig ist, sind Systeme zu verwenden, die keine oder nur in geringem Umfang personenbezogene Daten benötigen.

Zu § 8 (Verfahrensbeschreibung)

7. An die Stelle der Dateibeschreibung tritt die Verfahrensbeschreibung, die die aus der Anlage 1 ersichtlichen Punkte enthalten muss. Die Beschreibung erfolgt für das Verfahren und nicht für einzelne Dateien oder Verarbeitungsvorgänge. Soweit in bereichsspezifischen Vorschriften die Beschreibung einer automatisierten Datei gefordert ist, finden die Regelungen zur Verfahrensbeschreibung Anwendung (vgl. Nr. 2.3).

Verfahren zur Speicherung personenbezogener Daten zu einem anderen Zweck als der inhaltlichen Auswertung, für die keine Beschreibung zu erstellen ist, sind z.B. solche, die ausschließlich Zwecken der Datenschutzkontrolle, der Datensicherung oder der Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage dienen und bei denen nach der verarbeitungstechnischen Nutzung die personenbezogenen Daten gelöscht oder überschrieben werden. Als vorübergehend ist eine Speicherung anzusehen, wenn die Daten innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden.

Nicht unter die Beschreibungspflicht fallen Register nach § 8a Abs. 4. Nach der Verordnung über Ausnahmen von der Pflicht zur Bestellung von Datenschutzbeauftragten nach § 8a entfällt die Beschreibungspflicht für die Tätigkeit der Notarinnen und Notare sowie für die Verfahren zur Textverarbeitung einschließlich der Übermittlung elektronischer Dokumente über Telekommunikationsdienste an die Empfängerinnen und Empfänger.

Zu § 8a (Behördliche Datenschutzbeauftragte)

8.1 Grundsätzlich haben alle öffentlichen Stellen, die personenbezogene Daten automatisiert verarbeiten, Datenschutzbeauftragte zu bestellen, unabhängig von der Zahl der damit befassten Mitarbeiterinnen und Mitarbeiter. Außerhalb von Rechenzentren liegt eine automatisierte Datenverarbeitung vor, soweit Terminals zur Datenfernverarbeitung, Personalcomputer, Mehrplatzsysteme oder vernetzte Systeme zur Aufgabenerledigung eingesetzt werden.

Die Bestellung der oder des Beauftragten für den Datenschutz erfolgt durch die Leiterin oder den Leiter der Behörde oder sonstigen öffentlichen Stelle, bei der die Datenverarbeitungsanlagen oder die Datenendgeräte betrieben werden. Bestellt werden können auch Personen, die nicht der Daten verarbeitenden Stelle angehören, insbesondere können z.B. Gemeinden die Aufgaben einer oder eines Beauftragten für den Datenschutz Angehörigen der Kommunalen Datenzentralen übertragen. Es ist auch möglich, gemeinsam eine Beauftragte oder einen

Beauftragten für den Datenschutz zu bestellen. Werden bei einer Stelle Sozialdaten verarbeitet, gilt § 8a i.V.m. § 81 Abs. 4 Satz 4 SGB X.

Die Bestellung und ggf. auch Abberufung unterliegt gemäß § 67 Abs. 1 Nr. 9 NPersVG der Mitbestimmung des Personalrats.

8.2 Die oder der Beauftragte für den Datenschutz unterstützt die öffentliche Stelle bei der Sicherstellung des Datenschutzes und wirkt auf die Einhaltung der datenschutzrechtlichen Vorschriften hin.

Mit der Funktion sollen nicht Personen betraut werden, die dadurch in Interessenkonflikte geraten können, die über das unvermeidliche Maß hinausgehen; das wird in der Regel der Fall sein, wenn z.B. die Leiterin oder der Leiter von Rechenzentren oder Bedienstete der Systemverwaltung oder deren unmittelbare Vorgesetzten zur oder zum Beauftragten für den Datenschutz bestellt werden sollen. Die oder der Beauftragte für den Datenschutz hat vorrangig die Aufgabe, bei der Ausgestaltung der technischen und organisatorischen Maßnahmen nach § 7 zu beraten und auf die Durchführung der Maßnahmen sowie der Aufgaben nach § 8 hinzuwirken. Dabei hat sie oder er im Bereich der automatisierten Datenverarbeitung insbesondere

- auf der Grundlage des § 7 Abs. 2 zu prüfen, welche Maßnahmen zur Datensicherung erforderlich und angemessen sind,

- beim Erlass von Dienstanweisungen über getroffene bzw. zu treffende Datensicherungsmaßnahmen mitzuwirken,

- die Behördenleitung und die Beschäftigten aufgrund ihrer bzw. seiner Sachkenntnis in Fragen des Datenschutzes und der Datensicherung zu beraten und

- gegebenenfalls bei der Erledigung von Auskunftsbegehren nach § 16 mitzuwirken.

Damit die Beauftragten für den Datenschutz frühzeitig auf eine sachgerechte Ausgestaltung der Maßnahmen nach § 7 hinwirken können, sind sie bereits über geplante Verfahren zur automatisierten Verarbeitung personenbezogener Daten zu unterrichten.

8.3 Die Beauftragten für den Datenschutz haben auf Antrag, ohne dass es hierfür besonderer Voraussetzungen bedarf, jedermann die Verfahrensbeschreibungen, die ihnen von den Daten verarbeitenden Stellen zur Verfügung zu stellen sind, zugänglich zu machen. Über die Art und Form, z.B. Einsichtnahme oder kostenpflichtige Übersendung von Kopien, entscheiden die Beauftragten für den Datenschutz. Zulässig ist auch eine Veröffentlichung im Internet, wenn sichergestellt ist, dass sich die Informationen auf die Angaben zu den Nrn. 1 bis 6 der Verfahrensbeschreibungen (Seiten 1 bis 3 der Anlage 1 - ohne den behördeninternen Teil) beschränken und Informationen, die zu einer Beeinträchtigung der Verfahrenssicherheit führen könnten, nicht offenbart werden.

Gänzlich ausgenommen von dieser Verpflichtung sind Beschreibungen, wenn die Verarbeitungen der Erfüllung von Aufgaben nach dem NVerfSchG oder polizeilicher Aufgaben nach dem NGefAG oder zum Zweck der Strafverfolgung erfolgen.

Den Beauftragten für den Datenschutz obliegt die Vorabprüfung von Verfahren nach § 7 Abs. 3. Für die Durchführung hierfür notwendiger Erhebungen und Prüfungen können sie sich der Unterstützung der Daten verarbeitenden Stelle bedienen. Bei behörden- oder ressortübergreifenden Verfahren liegt die Zuständigkeit zur Vorabprüfung bei der oder dem Beauftragten für den Datenschutz der öffentlichen Stelle, die für die Einführung des Verfahrens verantwortlich ist.

8.4 Keine Beauftragten für den Datenschutz sind zu bestellen für öffentliche Stellen, die lediglich Register führen, die zur Information der Öffentlichkeit bestimmt sind und entweder jedermann oder allen Personen, die ein berechtigtes Interesse geltend machen, offen stehen. Nach der Verordnung über Ausnahmen von der Pflicht zur Bestellung von Datenschutz beauftragten nach § 8a entfällt die Pflicht zur Bestellung von Beauftragten für den Datenschutz für die Tätigkeit der Notarinnen und Notare sowie für die Verfahren zur Textverarbeitung einschließlich der Übermittlung elektronischer Dokumente über Telekommunikationsdienste an die Empfängerinnen und Empfänger.

Zu § 9 (Erhebung)

9.1 § 9 Abs. 1 Satz 3 nennt verschiedene Fälle, in denen Daten ohne Kenntnis der Betroffenen erhoben werden dürfen. Dazu gehört auch die Erhebung von Daten zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen gegenüber der Daten verarbeitenden Stelle, zur Rechnungsprüfung oder zur Durchführung von Organisationsuntersuchungen. Bei der Datenerhebung zu Ausbildungs- und Prüfungszwecken ist auch der in § 10 Abs. 3 Satz 2 enthaltende Gedanke (offensichtliches Überwiegen der berechtigten Interessen der Betroffenen an der Geheimhaltung der Daten) zu berücksichtigen.

Der Ausnahmetatbestand für die Datenerhebung aus allgemein zugänglichen Quellen (§ 9 Abs. 1 Satz 3 Nr. 5) ist mit der Einschränkung versehen, dass schutzwürdige Interessen der Betroffenen nicht offensichtlich entgegenstehen dürfen. Damit soll berücksichtigt werden, dass in Einzelfällen bei sensiblen persönlichen Daten die Rechtfertigung der Datenverarbeitung allein mit einer womöglich schon lange zurückliegenden - und vielleicht ihrerseits problematischen - Veröffentlichung bedenklich sein kann, wenn damit der Schutz der personenbezogenen Daten auf Dauer durchbrochen wird.

9.2 Für die in § 9 Abs. 2 geregelten Aufklärungs- und Unterrichtungspflichten bei der Datenerhebung bei Betroffenen ist anders als in § 4 Abs. 2 keine Schriftform vorgeschrieben. Gleichwohl sollte die Aufklärung in der Regel schriftlich erfolgen um die Betroffenen in die Lage zu versetzen ihre Rechte wahrnehmen zu können. Soweit Daten schriftlich erhoben werden, ist auch die Aufklärung in schriftlicher Form vorzunehmen. Eine besondere Unterrichtung über den Verwendungszweck ist nach § 9 Abs. 2 dann entbehrlich, wenn sich dieser aus den Gesamtumständen der Datenerhebung für Betroffene eindeutig erkennbar ergibt. Ein Verstoß gegen die Aufklärungspflichten macht die Datenerhebung nicht ohne Weiteres unwirksam und hindert die weitere Datenverarbeitung damit grundsätzlich nicht. Anders ist die

Rechtslage, wenn der Hinweis auf die Freiwilligkeit unterlassen wurde. In diesem Fall dürfen die erhobenen Daten nicht gespeichert werden, sie sind vielmehr von Amts wegen zu löschen (§ 17 Abs. 2 Nr. 1).

Im Rahmen des Hausrechts ist eine Beobachtung mit optisch-elektronischen Einrichtungen (Videoüberwachung) z.B. zur Sicherung von Dienstgebäuden zulässig, soweit nicht überwiegende schutzwürdige Interessen der Betroffenen dem entgegenstehen. Der Umstand der Beobachtung und der Zweck muss für die Betroffenen erkennbar sein (ggf. durch Anbringen von Hinweisschildern). Die dabei erhobenen Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer Speicherung entgegenstehen (§ 17 Abs. 2 Nr. 2).

Für öffentliche Stellen i.S. von § 2 Abs. 3 richtet sich die Zulässigkeit der Videoüberwachung nach § 6b BDSG.

Als spezielle bereichsspezifische, dem NDSG vorgehende Regelung ist § 32 Abs. 3 NGefAG anzusehen, der die Polizei und die Verwaltungsbehörden der Gefahrenabwehr ermächtigt, öffentlich zugängliche Orte mittels Bildübertragung offen zu beobachten, wenn dies zur Erfüllung von Aufgaben nach § 1 Abs. 1 NGefAG erforderlich ist.

Zu § 10 (Speicherung, Veränderung, Nutzung; Zweckbindung)

10.1 Nach § 10 Abs. 1 dürfen personenbezogene Daten nur für die Zwecke verarbeitet werden, für die sie erhoben oder - falls keine Erhebung vorausgegangen ist - erstmals gespeichert worden sind. Aufgrund dieses Zweckbindungsprinzips kommt der Festlegung des Verarbeitungszwecks für die Zulässigkeit der weiteren Verarbeitung der Daten eine zentrale Bedeutung zu (vgl. § 10 Abs. 2).

Werden Daten bei den Betroffenen erhoben, wird der Zweck durch die Aufklärung nach § 9 Abs. 2 Satz 1 begrenzt. Bei entsprechender Aufklärung können Daten auch gleichzeitig für unterschiedliche Zwecke erhoben werden.

Werden Daten in Ausführung einer Rechtsvorschrift verarbeitet, ergibt sich aus ihr auch der Zweck der Datenverarbeitung. Soweit in der Rechtsvorschrift keine besonderen Regelungen für die Verarbeitung personenbezogener Daten enthalten sind, kann in der Regel davon ausgegangen werden, dass es sich bei der Ausführung der Rechtsvorschrift insgesamt um einen Zweck und nicht verschiedene Zwecke i.S. des § 10 Abs. 1 und 2 handelt.

10.2 § 10 Abs. 2 Satz 2 enthält eine Sonderregelung für personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und der Daten verarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden sind.

Berufsgeheimnissen in diesem Sinne unterliegen die Angehörigen der in § 203 Abs. 1 StGB genannten Berufe. Zu den besonderen Amtsgeheimnissen gehören alle Geheimnisse, die aufgrund besonderer Rechtsvorschriften über das allgemeine Amtsgeheimnis, das seinen Ausdruck in § 30 VwVfG, den dienst- und arbeitsrechtlichen Verschwiegenheitspflichten und in § 5 gefunden hat, hinausgehen.

Hierzu gehören z.B. das Statistikgeheimnis, das Steuergeheimnis, das Post- und das Fernmeldegeheimnis.

10.3 Die Bearbeitung von Personalakten im Rahmen praxisgerechter Ausbildung hat in Abwägung mit den berechtigten Interessen der Betroffenen an der Geheimhaltung ihrer Daten zu erfolgen. Dabei sind folgende Punkte zu berücksichtigen:

Soweit möglich, ist es zu vermeiden, dass Auszubildende Personalakten von Bediensteten der Beschäftigungsbehörde bearbeiten, bei der die Auszubildenden später verbleiben. Stattdessen kommt z.B. die Ausbildung an Vorgängen nach geordneter Bereiche in Betracht, deren Bedienstete den Auszubildenden nicht persönlich bekannt sind. Wenn die Ausbildungspläne auch Stationen in anderen Behörden vorsehen, könnte eine Zuweisung in deren Personalstellen erfolgen.

Der Personalstellenleitung und der Ausbilderin oder dem Ausbilder obliegt es, ausbildungsfördernde Einzelfälle gezielt zur Bearbeitung zu übertragen; dabei ist darauf zu achten, dass besonders sensible Personalvorgänge nicht herangezogen werden.

Es sind nur die bearbeitungsrelevanten Personalakten bzw. Personalaktenteile zur Verfügung zu stellen; eine generelle Zugriffsmöglichkeit auf die Personalakten ist auszuschließen. Siehe auch Nr. 8.1 der VV zu § 101 NBG (Gern. RdErl. des MI, der StK und der übrigen Ministerien vom 25.11.1992, Nds. MBI. 1993 S. 93).

Zu § 10a (Automatisierte Einzelentscheidung)

11.1 Mit § 10a trifft der Gesetzgeber in Umsetzung der EG- Datenschutzrichtlinie eine grundsätzliche Wertentscheidung, nach der Betroffene nicht einer Entscheidung unterworfen werden sollen, die ausschließlich auf einer automatisierten Bewertung einzelner Persönlichkeitsmerkmale wie z.B. Zuverlässigkeit oder berufliche Leistungsfähigkeit beruht.

11.2 Damit Betroffene ihre Rechte wirksam ausüben können, erstreckt sich ihr Auskunftsanspruch auch auf den logischen Aufbau bzw. Art und Struktur der der automatisierten Einzelentscheidung zugrunde liegenden automatisierten Verarbeitung. Die Begriffe logischer Aufbau bzw. Art und Struktur der automatisierten Verarbeitung (vgl. § 16) sind inhaltsgleich und sollen deutlich machen, dass die Betroffenen darüber informiert werden müssen, nach welchen Entscheidungskriterien und Bewertungsmustern automatisierte Einzelentscheidungen ergehen.

Zu § 11 (Datenübermittlung innerhalb des öffentlichen Bereichs)

12. Für die Übermittlung personenbezogener Daten durch eine Weitergabe von Akten sieht § 11 Abs, 2 Verfahrenserleichterungen vor. Die Daten verarbeitende Stelle wird ihre Aktenführung allerdings so einrichten, dass eine Aktentrennung möglichst erreicht werden kann (z.B. vergleichbar der Regelung in Nr. 4.3 der VV zu § 101 NBG für die Personalaktenverwaltung). Ob ein unvertretbarer Aufwand vorliegt, kann in der Regel nur im Einzelfall entschieden werden. Die in § 11 Abs. 2 enthaltene Regelung gilt nicht für die automatisierte Verarbeitung personenbezogener Daten.

Zu § 12 (Automatisiertes Abrufverfahren)

13.1 Die Regelungen in § 12 gelten sowohl für bereits bestehende wie auch für geplante automatisierte Abrufverfahren unabhängig von der eingesetzten Technologie. So werden auch Abrufverfahren, die im Rahmen eines Internetangebots eingerichtet werden, mit erfasst. Die Regelungen finden jedoch keine Anwendung für die Einrichtung entsprechender Verfahren innerhalb einer öffentlichen Stelle. Hierbei ist anders als bei der Einrichtung automatisierter Abrufverfahren im Anwendungsbereich des SGB vom organisatorischen Behördenbegriff auszugehen. Geplante automatisierte Abrufverfahren sind der jeweils zuständigen obersten Landesbehörde mitzuteilen.

13.2 Soweit entsprechende Verfahren im Rahmen der Wahrnehmung von Aufgaben des übertragenen Wirkungskreises von Gemeinden, Landkreisen und sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts eingerichtet werden sollen, ist hierfür ebenfalls eine Verordnung erforderlich.

Sollen automatisierte Abrufverfahren zur Wahrnehmung von Aufgaben des eigenen Wirkungskreises eingerichtet werden, können diese nach § 12 Abs. 1 i.V.m. der satzungsbegründenden Rechtsvorschrift (z.B. § 6 NGO, § 5 NLO) durch Satzung zugelassen werden. Dabei sind die in § 12 Abs. 2 Sätze 3 und 4 enthaltenen Vorgaben zu berücksichtigen. Nach § 22 Abs. 1 ist die oder der Landesbeauftragte für den Datenschutz vor dem Erlass einer solchen Satzung anzuhören.

Zu § 13 (Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs)

14. Ein rechtliches Interesse nach § 13 Abs. 1 Satz 1 Nr. 2 liegt vor, wenn die Kenntnis der Daten für den Empfänger zur Verfolgung von Rechtsansprüchen oder Abwehr entsprechen der Forderungen erforderlich ist. Das berechtigte Interesse i.S. des § 13 Abs. 1 Satz 1 Nr. 3 umfasst darüber hinaus jedes private, ideelle oder vermögensweite Interesse, das von der Rechtsordnung als schutzwürdig anerkannt wird.

Zu § 14 (Übermittlung an Personen oder Stellen in Staaten außerhalb des Europäischen Wirtschaftsraums)

15.1 Auch wenn die in § 14 Abs. 1 Satz 1 genannten Voraussetzungen nicht vorliegen, ist eine Übermittlung personenbezogener Daten an Personen und Stellen in Staaten außerhalb des Europäischen Wirtschaftsraums unter den gleichen Voraussetzungen zulässig, die bei einer Datenübermittlung an Personen oder Stellen innerhalb des Europäischen Wirtschaftsraums (Inland, EU-Mitgliedsstaaten und die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum, zurzeit Norwegen, Island und Liechtenstein) zu beachten sind (vgl. § 11 Abs. 1 und § 13 Abs. 1), sofern im Empfängerland gleichwertige Datenschutzregelungen gelten. Als gleichwertig können Regelungen zur Gewährleistung eines Datenschutzstandards anerkannt werden, der zumindest dem entspricht, der sich aus der Verwirklichung der Grundsätze des Übereinkommens des Europarates über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (BGBl. 11 S. 538) ergibt. Dies gilt für Kanada, Israel, Ungarn, die

Schweiz sowie die Vereinigten Staaten von Amerika. Im Hinblick auf den Umfang der Ausnahmen nach Absatz 2 wird in der Praxis eine Prüfung, ob im Empfängerland gleichwertige Datenschutzbestimmungen gelten, nur in Ausnahmefällen erforderlich werden. Soweit im Einzelfall Zweifel bestehen, ob im Empfängerland gleichwertige Datenschutzregelungen gelten, ist dem MI zu berichten.

Ausländische Personen und nicht öffentliche Stellen sind entsprechend § 13 Abs. 2 zu verpflichten, die Daten nur für die Zwecke zu verarbeiten, zu denen sie ihnen übermittelt worden sind.

15.2 Unabhängig von dem Vorliegen gleichwertiger Datenschutzbestimmungen dürfen personenbezogene Daten übermittelt werden, soweit die Ausnahmen des Absatzes 2 vorliegen. Bei öffentlichen Registern muss in den Fällen der Nr. 3 Buchst. b die ausländische Person oder Stelle das berechtigte Interesse an der Einsichtnahme glaubhaft machen.

Zu § 15 (Übermittlung an Stellen öffentlich-rechtlicher Religionsgesellschaften)

16.1 § 15 enthält eine besondere Regelung für die Übermittlung personenbezogener Daten an Stellen öffentlich-rechtlicher Religionsgesellschaften. Die Übermittlung personenbezogener Daten an privatrechtliche Religionsgesellschaften ist unter den in § 13 genannten Voraussetzungen zulässig. Privatrechtlich organisierte Einrichtungen und Werke öffentlich-rechtlicher Religionsgesellschaften gehören nicht zu den in § 15 genannten Stellen; für die Übermittlung von Daten an diese gilt § 13.

Die Übermittlung personenbezogener Daten an Stellen öffentlich-rechtlicher Religionsgesellschaften nach § 15 Satz 1 Nrn. 3 bis 5 ist nur zulässig, wenn sichergestellt ist, dass bei den Empfängern ausreichende Datenschutzmaßnahmen getroffen sind. Bei den nachfolgend aufgeführten öffentlich-rechtlichen Religionsgesellschaften ist davon auszugehen, dass ausreichende Datenschutzmaßnahmen, insbesondere Regelungen zur Zweckbindung, getroffen sind. Im Übrigen sind die Voraussetzungen im Einzelfall zu prüfen.

16.1.1 Evangelische Landeskirchen
- Evangelisch-lutherische Landeskirche in Braunschweig,
- Evangelisch-lutherische Landeskirche Hannovers,
- Evangelisch-Lutherische Kirche in Oldenburg,
- Evangelisch-Lutherische Landeskirche Schaumburg-Lippe,
- Evangelisch-reformierte Kirche (Synode ev.-ref. Kirchen in Bayern und Nordwestdeutschland),
- Nordelbische Evangelisch-Lutherische Kirche,
- Bremische Evangelische Kirche,
- Ev. Kirche von Westfalen in Bezug auf die auf niedersächsischem Gebiet liegenden Teile von Kirchengemeinden.

16.1.2 Evangelisch-reformierte Gemeinden (außerhalb der Landeskirchen)
- Evangelisch-reformierte Gemeinde in Braunschweig,
- Evangelisch-reformierte Kirche in Bückeburg,
- Evangelisch-reformierte Gemeinde in Göttingen,
- Evangelisch-reformierte Kirche in Stadthagen.

16.1.3 Römisch-katholische Kirche
- Diözesen Hildesheim und Osnabrück, soweit sie zum Bereich des Landes Niedersachsen gehören,
- der oldenburgische Teil der Diözese Münster,
- die Kirchengemeinde Bad Pyrmont der Erzdiözese Paderborn.

16.1.4 Andere
- Katholische Pfarrgemeinde der Alt-Katholiken Hannover-Niedersachsen
- Landesverband der Jüdischen Gemeinden von Niedersachsen.

16.2 Soweit die Betroffenen in die Übermittlung personenbezogener Daten an Stellen öffentlich-rechtlicher Religionsgesellschaften eingewilligt haben oder eine bereichsspezifische Rechtsvorschrift die Datenübermittlung vorsieht, ist ebenfalls nicht zu prüfen, ob sichergestellt ist, dass bei diesen Stellen ausreichende Datenschutzmaßnahmen getroffen sind. Die Datenübermittlung ist dann bereits nach § 4 Abs. 1 Nr. 2 bzw. § 4 Abs. 1 Nr. 1, zweite Alternative zulässig.

Zu § 16 (Auskunft, Einsicht in Akten)

17.1 Eine Gefährdung der ordnungsgemäßen Wahrnehmung der sonstigen Aufgaben einer öffentlichen Stelle (§ 16 Abs. 4 Nr. 1) kann nur befristet einem Auskunftsoder Einsichtsverlangen entgegengehalten werden. In derartigen Fällen ist zu prüfen, ob nicht auch durch Teilauskünfte dem Verlangen zunächst Rechnung getragen werden kann. Auskunft ist auch darüber zu erteilen, ob die Daten verarbeitende Stelle personenbezogene Daten im Auftrag von anderen Stellen verarbeiten lässt. Soweit dies geschieht, erstreckt sich der Auskunftsanspruch auch auf die Nennung der Auftragnehmer.

Ob die Auskunft oder Akteneinsicht die öffentliche Sicherheit gefährdet oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde, wird von der Daten verarbeitenden Stelle nicht immer überblickt werden können. In Zweifelsfällen sind Stellungnahmen der zuständigen Behörden der Gefahrenabwehr, der Strafverfolgung oder des Verfassungsschutzes einzuholen.

17.2 Die Ablehnung eines Auskunfts- oder Akteneinsichtsverlangens ist zu begründen, soweit nicht der Ausnahmegrund des § 16 Abs. 5 Satz 1 vorliegt.

17.3 Für eine Auskunft oder Akteneinsicht sind weder Gebühren noch Auslagen zu erheben. Von der Kostenfreiheit nicht erfasst sind Leistungen, die über eine Auskunft oder Akteneinsicht hinausgehen und die nach allgemeinem Kostenrecht (VwKostG i.V.m. NVwKostG, AllGO) gebühren bzw. erstattungspflichtig sind, wie z.B. die Anfertigung von Ablichtungen, Entscheidungen im förmlichen Rechtsbehelfsverfahren.

Zu § 17 (Berichtigung, Löschung und Sperrung)

18.1 Bevor personenbezogene Daten nach § 17 Abs. 2 Satz 1 Nr. 2 gelöscht werden, haben die öffentlichen Stellen des Landes die Akten oder sonstigen Datenträger dem zuständigen Staatsarchiv zur Übernahme anzubieten (vgl. § 3 NArchG). Auf die speziellen Anbietungspflichten nach § 3 Abs. 6 Satz 1 und § 7 Abs. 3 NArchG wird hingewiesen.

Soweit für die Aufbewahrung von Akten nicht bereichsspezifische Aufbewahrungsfristen vorgeschrieben sind, ist die Löschung nach § 17 Abs. 2 Satz 1 Nr. 2 durchzuführen, wenn die in der Niedersächsischen Aktenordnung oder dem Niedersächsischen Aktenplan genannten Aufbewahrungsfristen abgelaufen sind.

Bei der Aussonderung von Akten oder sonstigen Datenträgern ist darauf zu achten, dass die erforderlichen technischen und organisatorischen Maßnahmen getroffen werden, um personenbezogene Daten insbesondere vor dem Zugriff Unbefugter zu schützen (§ 7 Abs. 1 und 4). Auch eine Zwischenlagerung des ausgesonderten Schriftguts bis zur Vernichtung muss diesen Anforderungen entsprechen.

Zur Vernichtung von Schriftgut kann eine öffentliche Stelle auch eine andere Behörde beauftragen, die einen Aktenvernichter besitzt. Sowohl bei der Beauftragung einer anderen öffentlichen Stelle wie auch eines privaten Unternehmens handelt es sich um einen Auftrag i.S. des § 6. Der Auftrag zur Löschung personenbezogener Daten, die Weisungen zu technischen und organisatorischen Maßnahmen sowie die Zulassung von Unterauftragsverhältnissen sind daher nach § 6 Abs. 2 Satz 2 schriftlich festzuhalten. Das Muster eines Vertrages über die Vernichtung von Altpapier durch einen Privatunternehmer ist als Anlage 2 beigefügt.

Für den Auftrag zur Vernichtung von Schriftgut mit Sozialdaten enthält § 80 SGB X eine bereichsspezifische Regelung.

18.2 Eine Unterrichtungspflicht gemäß § 17 Abs. 4 besteht nach dem Sinn der Regelung nicht, wenn die Daten gelöscht werden, weil ihre Kenntnis für die Daten verarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist (§ 17 Abs. 2 Satz 1 Nr. 2).

Zu § 17a (Widerspruchsrecht)

19. Mit § 17a wird den Betroffenen das Recht eingeräumt, einer rechtmäßigen Datenverarbeitung (§ 3 Abs. 2 Satz 1) zu widersprechen, soweit persönliche schutzwürdige Interessen einer Verarbeitung entgegenstehen und diese das Interesse der öffentlichen Stelle an der Verarbeitung der Daten überwiegen. Ausgenommen sind hier lediglich Verarbeitungen, die aufgrund gesetzlicher Vorschriften von der Daten verarbeitenden Stelle verpflichtend durchzuführen sind.

Zu § 18 Schadensersatz

20. § 18 sieht für die Verarbeitung personenbezogener Daten eine Gefährdungshaftung vor. Soweit die Daten nicht automatisiert verarbeitet werden, trifft die öffentliche Stelle die Ersatzpflicht nicht, wenn sie nachweist, dass die Unzulässigkeit der Datenverarbeitung nicht von ihr zu vertreten ist (Umkehr der Beweislast). Der oder dem Betroffenen obliegt der Nachweis der rechtswidrigen Verarbeitung und der Schadensverursachung.

Zu § 19 (Anrufung der oder des Landesbeauftragten)

21. Wird einem Hinweis einer oder eines Bediensteten auf einen Verstoß gegen datenschutzrechtliche Vorschriften nicht abgeholfen, so kann sich die oder der

Bedienstete nach § 19 Abs. 2 ohne Einhaltung des Dienstweges an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz wenden.

Zu § 22 (Aufgaben, Rechte und Pflichten der oder des Landesbeauftragten)

22. In folgenden Fällen ist die oder der Landesbeauftragte zu beteiligen:

- Unterrichtung über Planungen des Landes und der kommunalen Gebietskörperschaften zum Aufbau automatisierter Informationssysteme (§ 22 Abs. 2),

- Zulassung automatisierter Abrufverfahren nach § 12 Abs. 2 Satz 5,

- bei der Einrichtung automatisierter Dateien für Aufgaben nach dem NVerfSchG (§ 12) oder polizeilicher Aufgaben nach dem NGefAG (§ 46) durch Übersendung einer Ausfertigung der nach § 8 zu erstellenden Beschreibung (§ 22 Abs. 5),

- Anzeige der Übermittlung personenbezogener Daten an Personen oder sonstige nicht öffentliche Stellen sowie öffentlichen Stellen außerhalb des Geltungsbereichs des NDSG für Forschungsvorhaben (§ 25 Abs. 7 Satz 2),

- bei der Ausarbeitung von Gesetzentwürfen sowie beim Erlass von Verordnungen und Verwaltungsvorschriften des Landes, die Regelungen zum Recht auf informationelle Selbstbestimmung zum Gegenstand haben, ist die oder der Landesbeauftragte anzuhören,

- Unterrichtung über Gesetzesvorhaben (Referentenentwürfe) und den beabsichtigten Erlass von Verordnungen und Verwaltungsvorschriften des Bundes, soweit Regelungen über die Verarbeitung personenbezogener Daten vorgesehen sind und Stellen des Landes an der Erarbeitung entsprechender Entwürfe beteiligt werden.

Die Unterrichtungspflichten entbinden die Daten verarbeitenden Stellen nicht von ihrer Verantwortung für die datenschutzrechtliche Zulässigkeit der Maßnahmen. Diese ist in jedem Fall von den öffentlichen Stellen in eigener Zuständigkeit zu prüfen.

Zu § 25 (Verarbeitung personenbezogener Daten für Forschungsvorhaben)

23.1 Die in § 25 enthaltene bereichsspezifische Regelung für die Verarbeitung personenbezogener Daten für Forschungsvorhaben geht Regelungen für die Datenverarbeitung bei Dienst- und Arbeitsverhältnissen vor, so dass diese Daten im Rahmen der in § 25 festgelegten Voraussetzungen für Forschungsvorhaben verarbeitet werden dürfen.

23.2 § 25 Abs. 2 lässt unter den dort genannten Voraussetzungen abweichend von § 10 Abs. 2 die Weiterverarbeitung der schon von öffentlichen Stellen des Landes gespeicherten personenbezogenen Daten für wissenschaftliche Forschungsvorhaben zu.

Die in § 25 Abs. 2 Satz 1 Nr. 3 vorgeschriebene Abwägung zwischen den schutzwürdigen Interessen der Betroffenen und dem öffentlichen Interesse an der Durchführung des Forschungsvorhabens ist von der öffentlichen Stelle, die das Forschungsvorhaben durchführt, vorzunehmen.

Wird das Forschungsvorhaben von einer Privatperson, einer sonstigen nicht öffentlichen Stelle oder einer öffentlichen Stelle, die nicht in den Anwendungsbereich des NDSG fällt (z.B. eine öffentliche Stelle des Bundes oder eines anderen Bundeslandes), durchgeführt, ist die Abwägung nach § 25 Abs. 2 Satz 1 Nr. 3 von der übermittelnden Stelle vorzunehmen. Ergänzend hierzu sind die Empfänger in diesen Fällen nach § 25 Abs. 7 zu verpflichten, die Daten nur für das von ihnen bezeichnete Forschungsvorhaben und nach Maßgabe der Absätze 3 bis 5 zu verarbeiten.

23.3 § 25 Abs. 3 enthält eine besondere Zweckbindungsregelung, die den allgemeinen Zweckbindungsregelungen in § 10 Abs. 1 und 2 vorgeht. Eine Verarbeitung der für ein Forschungsvorhaben gespeicherten oder übermittelten Daten zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung oder zur Durchführung von Organisationsuntersuchungen ist jedoch zulässig, da hierin keine zweckändernde Verarbeitung liegt (§ 10 Abs. 3 Satz 1).

23.4 Werden personenbezogene Daten an eine andere als eine öffentliche Stelle des Landes für ein Forschungsvorhaben übermittelt, ist die Übermittlung der oder dem Landesbeauftragten nach § 25 Abs. 7 Satz 2 von der übermittelnden Stelle vorher so rechtzeitig anzuzeigen, dass die oder der Landesbeauftragte zu der Zulässigkeit der Datenübermittlung gegebenenfalls noch Stellung nehmen kann.

Zu § 28 (Straftaten)

24. Mit der Änderung, dass bei der Strafbarkeit künftig auf die unbefugte Verarbeitung von "Daten, die nicht allgemein zugänglich sind" abstellt wird, soll der Rechtsprechung mehrerer Strafgerichte (z.B. Bay0bLG NJW 1999, S. 1727) Rechnung getragen werden, die das bisherige Merkmal "offenkundig" für die Kfz-Halter-Datei bejaht und daher Personen, die daraus Daten weitergegeben hatten, freigesprochen haben. Auf der Grundlage dieser Rechtsauffassung konnten z.B. unbefugte Abrufe aus dem zentralen Informationssystem des Kraftfahrtbundesamtes durch einzelne öffentliche Bedienstete und die Weitergabe dieser Daten an private Stellen strafrechtlich nicht geahndet werden. Durch die Änderung des Gesetzes soll sichergestellt werden, dass bei Vorliegen der sonstigen Voraussetzungen des § 28 eine strafrechtliche Ahndung nur in denjenigen Fällen ausgeschlossen ist, in denen es sich um Daten handelt, die von jedermann zur Kenntnis genommen werden können, ohne dass der Zugang aus Gründen des Persönlichkeitsschutzes rechtlich beschränkt ist.

Entsprechendes gilt für die Änderung der Regelung in § 29 (Ordnungswidrigkeiten).

Zu § 29 (Ordnungswidrigkeiten)

25. Die Ahndung der Ordnungswidrigkeiten richtet sich bei Zuwiderhandlungen von Beschäftigten nach § 6 Nr. 9 ZustVO-OWi, im Übrigen gilt die Regelzuständigkeit.

Schlussbestimmungen

26.1 Den Gemeinden, Landkreisen und den sonstigen der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen wird empfohlen, entsprechend zu verfahren.

26.2 Der Bezugserlass wird aufgehoben.

Anlage 1 Verfahrensbeschreibung gemäß § 8 NDSG

Anlage 2

(Muster)

Vertrag über die Übernahme und Vernichtung von ausgesondertem Schriftgut (EDV-Papier und Aktenmaterial)

Zwischen ..... ,

im Folgenden Auftraggeber genannt,

und der Firma ..... wird folgender Vertrag geschlossen:

§1

Der Vertrag regelt die Übernahme und Vernichtung von ausgesondertem Schriftgut.

§2

Die Vertragsfirma verpflichtet sich zur ordnungsgemäßen Übernahme und Vernichtung des Schriftgutes.

§3

Die Abholung erfolgt nach Terminvereinbarung. Es darf grundsätzlich nur so viel Schriftgut abgeholt werden, wie am selben Tag restlos vernichtet werden kann. Die oder der zur Übernahme des Schriftgutes Berechtigte übergibt als Berechtigungsnachweis ein vorgefertigtes Übernahmeprotokoll. Übergabe und Übernahme bestätigen beide Seiten auf dem Protokoll. Von der Übergabe des zu vernichtenden Schriftgutes an haftet die Vertragsfirma für den sicheren Transport und die ordnungsgemäße Vernichtung.

§4

Der Transport darf nur in geschlossenen Fahrzeugen (ordnungsgemäß befestigte Planen usw. oder Container) durchgeführt werden, so dass kein Material verloren gehen kann.

§5

(1) Das übernommene Schriftgut wird von der Vertragsfirma am selben Tag vernichtet. Nur in Ausnahmefällen darf das zu vernichtende Schriftgut über Nacht in verschlossenen Räumen abgestellt werden, zu denen Unbefugte keinen Zutritt haben.

(2) Als vernichtet gilt Schriftgut, wenn es so zerkleinert oder zusammengepresst ist, dass zusammenhängende Sätze, Wörter oder Zahlenkolonnen nicht zu rekonstruieren sind. Dazu ist das Schriftgut mindestens gemäß Sicherheitsstufe ..... der DIN 32757-1 zu zerkleinern. Außerdem sind folgende zusätzliche Maßnahmen zur Vernichtung durchzuführen:

[_] Verwirbelung [_] Verpressung [_] Abgabe an eine Papierfabrik [_] Sonstiges

(3) Die Vertragsfirma hat über die Vernichtung des Schriftgutes eine schriftliche Bestätigung abzugeben.

§6

Die Vertragsfirma verpflichtet sich, den in ihrem Betrieb beschäftigten Personen jedes Beiseiteschaffen von Schriftgut so wie die Einblicknahme in Schriftgut zu verbieten und die Einhaltung dieser Anordnung zu überwachen.

§7

(1) Der Transport und die Vernichtung des Schriftgutes können vom Auftraggeber oder von einer von ihr benannten Stelle überwacht oder kontrolliert werden.

(2) Die Vertragsfirma verpflichtet sich die Anwesenheit einer Mitarbeiterin/eines Mitarbeiters des Auftraggebers oder der von dem Auftraggeber benannten Stelle bei allen mit dem Transport und der Vernichtung zusammenhängenden Dienstleistungen und in allen dabei benutzten Räumen, Fahrzeugen und Betriebseinrichtungen zu dulden. Dabei ist der Betriebsablauf so zu gestalten, dass die Überwachung durch die Aufsichtsperson jederzeit gewährleistet ist.

§8

Bei Nichtbeachtung der in diesem Vertrag übernommenen Verpflichtungen, insbesondere bezüglich der Geheimhaltung des Inhalts des Schriftgutes, bei Erschwerung der Überwachung oder bei nicht rechzeitiger Vernichtung des

übernommenen Schriftgutes ist der Auftraggeber berechtigt, unverzüglich und ohne Entschädigung den Vertrag zu kündigen.

§9

Ansprechpartnerin/Ansprechpartner für Meldungen von Unregelmäßigkeiten bei der Abwicklung von Arbeiten sind

für den Auftraggeber .....

und für die Vertragsfirma .....

§10

(Entgeltvereinbarungen und Verwertungsvereinbarungen sind nach den jeweiligen Erfordernissen in den Vertrag aufzunehmen. Bis zur vollständigen Vernichtung ist das Eigentum des Auftraggebers an dem Schriftgut vorzubehalten.)

(Vertragsdauer und Gerichtsstand)