

Eckpunktepapier

zur Änderung des Niedersächsischen Datenschutzgesetzes

Zusammenfassung

In den letzten Jahren hat sich die Nutzung der Informations- und Telekommunikationstechnik (IT) durch öffentliche Stellen rasant weiterentwickelt: Allein die alltägliche Nutzung von Internet und E-Mail-Diensten sowie Überwachungen mittels Videokameras sind heutzutage nicht mehr wegzudenken. Umfangreiche Neuorganisationen der Behörden sowie die Ausweitung der (länderübergreifenden) Zusammenarbeit auf Grund von EU-Richtlinien oder im Rahmen der interkommunalen Zusammenarbeit haben aufgezeigt, dass es u. a. der Umsetzung einheitlicher technischer Standards bedarf. Den Belangen des Datenschutzes wurde bei diesen Neustrukturierungen oder beim Einsatz der IT-Technik oftmals nicht ausreichend Rechnung getragen. Unter Datenschützern besteht weitgehend Einigkeit, dass das geltende Datenschutzrecht die Zielvorstellungen der Übersichtlichkeit und Verständlichkeit, der Angemessenheit der Problemlösungen und der Akzeptanz gerade angesichts der stürmischen Entwicklung der Datenverarbeitungstechnik noch längst nicht - oder nicht mehr - hinreichend erfüllt.

Oftmals wird nicht beachtet, dass der Datenschutz nicht nur eine Schutzfunktion hat, sondern auch einen Gestaltungsanspruch der Betroffenen beschreibt: Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß. Datenschutz ist Grundrechtsschutz und die Wahrung der informationellen Selbstbestimmung ist eine Funktionsbedingung einer menschenwürdigen Informationsgesellschaft.

Ich verweise auf die EntschlieÙung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Sitzung am 17./18. März 2010) „Ein modernes Datenschutzrecht für das 21. Jahrhundert“, in der Eckpunkte für eine Diskussion zur Reform des Datenschutzrechts zusammengefasst worden sind.

Das seit 1993 bestehende Niedersächsische Datenschutzgesetz (NDSG) wurde zuletzt im Jahre 2001 grundlegend überarbeitet, 2004 wurde der § 25 a NDSG „Beobachtung durch Bildübertragung“ eingefügt. Im Juli 2011 wurden mit dem Gesetz zur Neuregelung der Rechtsstellung der oder des Landesbeauftragten für den Datenschutz die Forderungen des Europäischen Gerichtshofs (Urteil vom 09. März 2010 - C-518/07 -) zur Unabhängigkeit der Aufsichtsstellen für den Datenschutz mittels Änderung der Niedersächsischen Verfassung sowie des NDSG und weiterer Gesetze entsprochen. Im Dezember 2012 wurde der § 24 NDSG „Datenverarbeitung bei Dienst- und Arbeitsverhältnissen“ eingefügt.

Mit der vorliegenden Fassung des Gesetzes ist die Entwicklung des Datenschutzrechts selbstverständlich nicht abgeschlossen. Die Erfahrungen der Vergangenheit haben gezeigt, dass die bestehenden Rechtsgrundlagen oftmals nicht ausreichen oder zu unbestimmt sind. Das NDSG bedarf der Modernisierung. Als Grundlage für eine Diskussion über eine Reform des NDSG sind hier die wichtigsten Eckpunkte zusammengefasst:

- **Verankerung konkreter Schutzziele und Grundsätze, Schaffung eines technikneutralen Ansatzes**
- **Stärkung der Eigenkontrolle der verantwortlichen Stellen**
- **Stärkung der Datenschutzaufsicht**
- **Aktualisierung des geltenden Rechts**

Die notwendigen redaktionellen Änderungen bleiben dabei unberücksichtigt.

Inhaltsverzeichnis:

	Seite
1.1 Zielbestimmungen und Grundstruktur des NDSG (Allgemeine Grundregelungen, § 7 NDSG).....	4
1.2 Anwendungsbereich des NDSG (§ 2 NDSG).....	4
1.3 Stärkung der Stellung des behördlichen Datenschutzbeauftragten (§ 8 a NDSG).....	5
1.4 Beteiligung mehrerer Stellen an der Datenverarbeitung / Cloud Computing (Neue Regelung „Gemeinsame Verfahren“).....	6
1.5 Automatisierte Abrufverfahren (§ 12 NDSG).....	7
1.6 Eigenkontrolle der verantwortlichen Stellen (Neue Regelung).....	8

1.1 Zielbestimmungen und Grundstruktur des NDSG

Das Bundesverfassungsgericht hat nach dem Volkszählungsurteil im Jahre 1983 in späteren Urteilen die Bedeutung des Grundrechts der informationellen Selbstbestimmung immer wieder unterstrichen, den Datenschutz verfassungsrechtlich weiter gestärkt und ihn an die Herausforderungen des elektronischen Zeitalters angepasst. So hat es z. B. in seiner Entscheidung vom 27. Februar 2007 - 1 BvR 370/07, 1 BvR 595/07 - festgestellt, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. Neben dem rechtlichen Schutz der personenbezogenen Daten ist auch eine angemessene Datensicherheit zu gewährleisten.

Im NDSG sollten diese allgemeinen Grundregelungen stärker verankert werden. Hierfür sind Gestaltungsregeln erforderlich, die dem Stand der Technik entsprechen. Z. B. stammen die bisher in § 7 Abs. 2 NDSG beschriebenen technisch organisatorischen Kontrollmaßnahmen im Kern aus der Zeit der Großrechner, in der Personalcomputer und Internet noch unbekannt waren. Der Datenschutz war geprägt von der Vorstellung einer monolithischen Großrechnerwelt und primär verbunden mit dem Schutz der Rechner, die in hermetisch abgeschlossenen Rechenzentren betrieben wurden. Die rasante Entwicklung der Informations- und Kommunikationstechnik hat heute die schnelle Verarbeitung großer Datenmengen, eine weltweite Kommunikation in digitalen Netzen ohne Grenzen und Zeitverzug sowie die jederzeitige Erreichbarkeit an allen Plätzen der Welt möglich gemacht. Datensicherung ist heute nicht mehr an technischen Anlagen festzumachen, sondern – im eigentlichen Sinne des Wortes – an den Daten selbst.

Heutige Gestaltungsziele der informationstechnischen Sicherheit sind u. a. Vertraulichkeit und Integrität, auch informationstechnischer Systeme, sowie Verfügbarkeit und Authentizität. Sie werden ergänzt um die Gebote zur datensparsamen Verfahrensgestaltung sowie zur Transparenz und Revisionsfähigkeit der Verfahren. Diese modernen Sicherheitsziele sind technologieunabhängig; sie stellen einen allgemein gültigen Sicherheitsrahmen dar, der auch bei neuen Formen der Datenverarbeitung Bestand haben wird.

Auf die o. g. EntschlieÙung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ wird verwiesen.

1.2 Anwendungsbereich des NDSG

Die Regelungen des § 2 Abs. 1 Satz 1 sowie des Absatzes 3 Nr. 1 und Abs. 4 NDSG führten in den letzten Jahren vermehrt zu Anfragen von Vereinigungen und Unternehmen (insbesondere von Gesellschaften mit beschränkter Haftung (GmbH)) des Landes bzw. im kommunalen Bereich, welches Recht sie anzuwenden haben und warum einzelne Unternehmen nebeneinander zwei Gesetze zu beachten haben (BDSG und NDSG):

Gemäß § 2 Abs. 1 NDSG gilt für die Datenverarbeitung von Behörden und sonstigen öffentlichen Stellen Niedersachsens und deren Vereinigungen ohne Rücksicht auf den rechtlichen Charakter ihrer Tätigkeit das NDSG.

Eine Vereinigung in diesem Sinne liegt allerdings nur vor, wenn sie von mehreren öffentlich-rechtlichen Trägern gebildet wird. Deshalb spricht Satz 1 von „deren“ Vereinigungen. Eine nur von einem Rechtsträger gebildete Vereinigung (z. B. eine GmbH des Landes oder einer Gemeinde) fällt nicht in den Anwendungsbereich des NDSG: Hier gelten die Vorschriften des BDSG. Es bedarf also im Einzelfall der Prüfung der Trägerschaft.

Die in § 2 Abs. 3 Satz 1 Nr. 1 NDSG genannten juristischen Personen des öffentlichen Rechts oder deren organisatorisch selbständigen Einrichtungen, die am Wettbewerb teilnehmen, sog. „öffentliche Wettbewerbsunternehmen“, sind von der Geltung des NDSG weitgehend ausgenommen: Auf die Datenverarbeitung von „öffentlichen Wettbewerbsunternehmen“ finden grundsätzlich die Vorschriften des BDSG Anwendung, dies gilt jedoch nur, soweit personenbezogene Daten „in Ausübung wirtschaftlicher Tätigkeit“ verarbeitet werden. Rechtsgrundlage für die Datenverarbeitung bei Dienst- und Arbeitsverhältnissen von Mitarbeiterinnen und Mitarbeitern dieser Wettbewerbsunternehmen ist in Niedersachsen das NDSG, dem allerdings bereichsspezifische Regelungen vorgehen (vgl. § 2 Abs. 6 NDSG).

Für viele Vereinigungen und Unternehmen ist die auf Grund des Wortlauts des Gesetzes vorzunehmende Unterscheidung nicht nachvollziehbar. So führt die derzeit bestehende Rechtslage z. B. zu der misslichen Situation, dass „öffentliche Wettbewerbsunternehmen“ sowohl das BDSG als auch das NDSG zu beachten und einen betrieblichen sowie einen behördlichen Datenschutzbeauftragten (auch wenn die Bestellung in einer Person in Betracht kommt) zu bestellen haben. Diesbezüglich ist an mich der Wunsch

nach einer eindeutigen gesetzlichen Regelung herangetragen worden, die von mir unterstützt wird.

1.3 *Stärkung der Stellung des behördlichen Datenschutzbeauftragten*

Eine wirksame Aufgabenwahrnehmung durch die behördlichen Datenschutzbeauftragten erfordert, dass diese, sofern sie diese Aufgabe nicht hauptamtlich ausüben, im jeweils erforderlichen Umfang von anderen Tätigkeiten entlastet werden. Vor dem Hintergrund, dass der Aufgabenbestand der Datenschutzbeauftragten durch die zunehmenden E-Government-Verfahren erheblich ausgeweitet wurde, reicht es künftig aus meiner Sicht nicht mehr aus, diese Aufgabe einer/einem Beschäftigten zusätzlich zu seinen sonstigen Aufgaben ohne angemessene Freistellung zu übertragen. Zwar hat der Gesetzgeber der Forderung, in das Gesetz einen Rechtsanspruch auf Freistellung im erforderlichen Umfang aufzunehmen, auch im Hinblick auf die Organisationshoheit der Kommunen nicht entsprochen. In der Gesetzesberatung bestand jedoch Einvernehmen darüber, dass den Datenschutzbeauftragten angemessene zeitliche Ressourcen zur Verfügung stehen müssen, um ihre Aufgabe wirksam ausüben zu können.

Die Rückmeldungen aus der Praxis zeigen auf, dass die verantwortlichen Stellen die behördlichen Datenschutzbeauftragten aber oftmals nicht ausreichend von ihren sonstigen Aufgabenbereichen freistellen. Eine Umfrage des Netzwerkes NORDWEST (Zusammenschluss der behördlichen Datenschutzbeauftragten der Kommunen) im letzten Jahr hat ergeben, dass den kommunalen Datenschutzbeauftragten eine wirksame Aufgabenwahrnehmung im gesetzlich geforderten Umfang oftmals nicht möglich ist: Viele Datenschutzbeauftragte, die die Aufgabe nicht hauptamtlich ausüben, erfahren gerade nicht die Entlastung im jeweils erforderlichen Umfang von anderen Tätigkeiten.

Mangels gesetzlicher Regelung vermag ich gegenüber den behördlichen Datenschutzbeauftragten nur darauf hinzuweisen, schriftlich aufzulisten, welche Aufgaben mit welchen Zeitanteilen im Laufe eines gewissen Zeitraums anfallen, um bei Bedarf einen Nachweis ihrer Tätigkeiten vorlegen zu können. Um den zuständigen politischen Gremien verdeutlichen zu können, welche Aufgabenbereiche den behördlichen Datenschutzbeauftragten obliegen und wie zeitintensiv sich viele Projekte gestalten, wäre z. B. eine gesetzliche Verpflichtung für die behördlichen Datenschutzbeauftragten zur jährlichen Vorlage eines (Tätigkeits-)berichts sinnvoll. Zur Vergleichbarkeit der Berichte sollten Mindestanforderungen für den Bericht festgelegt werden (Muster).

In meinem XIX. Tätigkeitsbericht 2007/2008 habe ich unter dem Titel „Zusammenarbeit mit den kommunalen Datenschutzbeauftragten“ (vgl. Abschnitt 1, Datenschutz im öffentlichen Bereich, S. 6 der Broschüre) bereits auf diese Problematik hingewiesen. Die bestehende Regelung sollte diesbezüglich überdacht werden.

Außerdem sollten im Hinblick auf die im BDSG vorgenommenen Änderungen zur Stärkung der Stellung der betrieblichen Datenschutzbeauftragten im Hinblick auf den Gleichbehandlungsgrundsatz auch im NDSG ergänzende Regelungen aufgenommen werden.

1.4 *Beteiligung mehrerer Stellen an der Datenverarbeitung / Cloud Computing*

Das NDSG beinhaltet keine ausdrückliche Regelung für eine gemeinsame Verarbeitung personenbezogener Daten durch mehrere Stellen. § 12 NDSG regelt lediglich den automatisierten Abruf von Daten durch Dritte.

Anders als in der europäischen Datenschutzrichtlinie kennt das NDSG beim Begriff der verantwortlichen Stelle nicht die Möglichkeit einer gemeinsamen Verantwortlichkeit mehrerer Stellen („joint controllership“). In der Praxis kommt zentralen IT-Verfahren eine wachsende Bedeutung zu, an denen z. B. verschiedene Stellen von Bund und Ländern, mehrerer Länder oder gar nicht-öffentliche Stellen beteiligt sind.

Es ist außerordentlich schwierig, solche Verfahren gesetzeskonform zu betreiben, weil die klassischen Instrumente Auftragsdatenverarbeitung oder Übermittlung nicht passen und zudem völlig unterschiedliche und z. T. einander widersprechende datenschutzrechtliche Normen des Bundes und der Länder beachtet werden müssten. Außerdem sind u. U. zahlreiche Kontrollbehörden für die datenschutzrechtliche Kontrolle nebeneinander zuständig.

Weitere Fragen wirft auch die verteilte und häufig grenzüberschreitende Datenverarbeitung auf, wie es z. B. beim Cloud Computing oder beim Binnenmarktinformationssystem (IMI) der Fall ist. Solche Konstellationen sind mit dem Datenschutzrecht nicht befriedigend in Einklang zu bringen. Das Instrument der Auftragsdatenverarbeitung lässt sich in der Praxis nicht umsetzen. Legt man die Funktionsübertragung (mit Übermittlung von Daten zwischen den beteiligten Stellen) zugrunde, ist die Verteilung der Verantwortlich-

keiten nicht befriedigend zu regeln. Aus diesen Gründen sollte das Konzept der Zuweisung von Verantwortlichkeiten neu gefasst werden.

- Der Begriff der verantwortlichen Stelle ist an dem Vorbild von Art. 2 lit. d) der EG-Datenschutzrichtlinie zu orientieren.
- Die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung ist bei der Beteiligung mehrerer Stellen durch entsprechende Vorschriften von den tatsächlichen Einflussmöglichkeiten und der Interessenlage abhängig zu machen (Prinzip der „Accountability“). Die datenschutzrechtliche Verantwortlichkeit kann demnach z. B. auch nach einer Übermittlung fortbestehen, wenn die wirtschaftlichen bzw. tatsächlichen Einwirkungsmöglichkeiten auf die Empfänger vorhanden sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat für Verfahren, die mehreren Stellen die gemeinsame Verarbeitung personenbezogener Daten ermöglichen (gemeinsame Verfahren) bereits einen konkreten Vorschlag für eine gesetzliche Formulierung entwickelt, der angepasst auf bereits bestehende Regelungen des NDSG wie folgt lautet:

„Gemeinsame Verfahren

(1) ¹Automatisierte Verfahren, die mehreren Stellen die Verarbeitung personenbezogener Daten in oder aus einem Datenbestand ermöglichen (gemeinsame Verfahren), sind nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. ²Gemeinsame Verfahren von erheblicher Bedeutung sind durch Gesetz oder Staatsvertrag zu regeln. ³Gemeinsame Verfahren sind auch Verfahren, die die Übermittlung von Daten einer Stelle durch Abruf einer oder mehrerer anderer Stellen ermöglichen. ⁴Die Vorschriften über die Zulässigkeit der Verarbeitung der Daten im Einzelfall bleiben unberührt. ⁵Vor der Einrichtung oder wesentlichen Änderung eines gemeinsamen Verfahrens ist eine Vorabkontrolle (§ 7 Abs. 3 NDSG) zu erstellen und der oder die Landesbeauftragte für den Datenschutz zu hören. ⁶Ihm oder ihr sind die Festlegungen nach Abs. 2 und das Ergebnis der Vorabkontrolle vorzulegen.

(2) Vor der Einrichtung eines gemeinsamen Verfahrens ist über die Angaben nach § 8 NDSG hinaus schriftlich insbesondere

1. *die Verfahrensweise und die jeweils verantwortliche Stelle für die Festlegung, Änderung, Fortentwicklung und Einhaltung von fachlichen und technischen Vorgaben für das gemeinsame Verfahren zu bestimmen und*
2. *zu dokumentieren, welche der beteiligten Stellen jeweils für die Rechtmäßigkeit der Datenverarbeitung verantwortlich ist.*

Die nach Nr. 1 verantwortlichen Stellen bestimmen eine Stelle, die ein Doppel des von den beteiligten Stellen zu erstellenden Verfahrensverzeichnisses verwahrt und es nach § 8a Abs. 3 NDSG zusammen mit den Angaben nach Nr. 1 und 2 zur Einsicht für jeden bereit hält.

Nach Satz 1 Nr. 1 können auch verantwortliche Stellen bestimmt werden, die andere Stellen mit der Verarbeitung personenbezogener Daten für das gemeinsame Verfahren beauftragen dürfen. Die Vorschriften zur Auftragsdatenverarbeitung bleiben im Übrigen unberührt.

(3) Soweit für die beteiligten Stellen unterschiedliche Datenschutzvorschriften gelten, ist zu regeln, welches Datenschutzrecht zur Anwendung kommen soll. Weiterhin ist zu bestimmen, welche Kontrollstellen die Einhaltung der Datenschutzvorschriften prüfen.

(4) Die Betroffenen können ihre Rechte nach § 8a Abs. 3 Satz 4 NDSG gegenüber jeder der beteiligten Stellen geltend machen unabhängig davon, welche Stelle im Einzelfall für die Verarbeitung der betroffenen Daten nach Abs. 2 Nr. 2 verantwortlich ist. Die Stelle, an die der Betroffene sich wendet, leitet das Anliegen an die jeweils zuständige Stelle weiter.“

1.5 Automatisierte Abrufverfahren

Nach § 12 NDSG ist die Einrichtung automatisierter Abrufverfahren (= Übermittlung personenbezogener Daten durch Abruf eines Dritten) nur durch Rechtsvorschrift zugelassen. Das Erfordernis einer speziellen Rechtsgrundlage für einzelne Abrufverfahren ist in Anbetracht der zunehmenden Bedeutung automatisierter Verfahren, u. a. im Rahmen der interkommunalen Zusammenarbeit, nicht mehr praxismäßig. Es sollte überlegt werden, § 12 NDSG so zu ändern, dass die Vorschrift als eigenständige Befugnisnorm für automatisierte Abrufverfahren gilt. Ähnlich der Regelung des § 79 SGB X sollten in § 12 NDSG lediglich die Voraussetzungen für die Zulässigkeit des Abrufverfahrens festgelegt werden. Es bedarf dann keiner gesonderten Rechtsvorschrift für die diversen Fachbereiche mehr, sondern lediglich der schriftlichen Festlegung bestimmter Eckpunk-

te, wie z. B. von Kontrollrechten und notwendiger technischer und organisatorischer Maßnahmen.

1.6 Eigenkontrolle der verantwortlichen Stellen

Im NDSG ist das Verbotssprinzip verankert, d. h., die Verarbeitung personenbezogener Daten und deren Nutzung sind grundsätzlich verboten (vgl. § 4 Abs. 1 NDSG), Kontroll- und Sanktionsmaßnahmen bei festgestellten Verstößen obliegen den behördlichen Datenschutzbeauftragten bzw. dem Landesbeauftragten für den Datenschutz (vgl. § 7 Abs. 3, § 25a Abs. 6, § 22, § 23, § 28 und § 29 NDSG). Auf Grund sehr geringer Kontrollichte führt dies zu erheblichen Vollzugsdefiziten. Ein modernes Datenschutzrecht muss deswegen die Elemente der Eigenkontrolle stärken. Datenschutz muss von den verantwortlichen Stellen als eigenes Anliegen begriffen werden und nicht nur als von außen aufgezwungene Beschränkung. Daneben müssen interne Mechanismen bei den verantwortlichen Stellen entwickelt und gestärkt werden, die die Einhaltung des Datenschutzes sicherstellen, ohne dass es einer ständigen Kontrolle von außen bedarf.

Eine neu aufzunehmende gesetzliche Verpflichtung der verantwortlichen Behörden und öffentlichen Stellen, für ihre Verarbeitung personenbezogener Daten ein Datenschutz- und Datensicherheitskonzept zu entwickeln, würde diese zwingen, sich mit der Thematik auseinanderzusetzen, Schwachstellen aufzudecken und entsprechende Vorkehrungen zu treffen.

Der Landesbeauftragte für den Datenschutz Niedersachsen

Prinzenstr. 5

30159 Hannover

Tel.: 0511 120 - 4500

Fax: 0511 1204599

E-Mail: poststelle@lfd.niedersachsen.de

Stand: 27. Dezember 2013