**Antwort auf eine Kleine schriftliche Anfrage**
- Drucksache 17/1936 -

Wortlaut der Anfrage der Abgeordneten Dr. Marco Genthe, Jan-Christoph Oetjen und Jörg Bode (FDP), eingegangen am 04.09.2014

**No-Spy-Garantie für künftige IT-Aufträge?**

Über ein Jahr ist es inzwischen schon her, dass der NSA-Abhörskandal durch den ehemaligen Mitarbeiter des amerikanischen Geheimdienstes Edward Snowden aufgedeckt wurde. Seitdem werden regelmäßig neue Praktiken und Programme der NSA und auch anderer Geheimdienste veröffentlicht. Demnach haben einige Landesverwaltungen in den letzten Jahren mit IT-Firmen zusammengearbeitet, die im Zuge dieses Skandals aufgefallen sind und die Kundeninformationen an britische und amerikanische Geheimdienste übermittelt haben. Aus diesem Grund fordert die Bundesregierung (laut einigen Medienberichten) schon seit längerer Zeit eine No-Spy-Garantie für die Vergabe von IT-Aufträgen. Dabei sollen die Unternehmen vor Auftragsvergabe zusichern, dass sie verantwortungsvoll mit den Daten umgehen und diese nicht weiterleiten werden.

Vor diesem Hintergrund fragen wir die Landesregierung:

1. Wie bewertet die Landesregierung die Forderung nach einer solchen No-Spy-Garantie?
2. Inwiefern gibt es in Niedersachsen schon Bemühungen, die dafür sorgen sollen, dass vertrauensvoll mit den Kundeninformationen umgegangen wird?
3. Inwiefern besteht aus Sicht der Landesregierung bezogen auf diese Thematik die Notwendigkeit für eine bundesweite Lösung?
4. Wo und bei welchen Firmen sind Daten der Landesverwaltung auf welchen Datenträgern (z. B. Server oder Cloud) gespeichert, und inwiefern kann die Landesregierung in einem solchen Fall Datenmissbrauch ausschließen und sicherstellen, dass an diesen Standorten deutsche Standards eingehalten werden?

(An die Staatskanzlei übersandt am 15.09.2014)

**Antwort der Landesregierung**

Niedersächsisches Ministerium
für Inneres und Sport
- 42.20-01425/0001-0010 -

Hannover, den 27.11.2014

In den Behörden der niedersächsischen Landesverwaltung wird Informationstechnologie in vielfältiger Weise zur Aufgabenerfüllung genutzt. Hierbei ist es ein besonderes Anliegen der Landesregierung, die Vertraulichkeit, Verfügbarkeit und Integrität aller Daten, die zur Aufgabenerfüllung der öffentlichen Verwaltung verarbeitet werden, sicherzustellen.

Bereits im Jahr 2011 hat der Niedersächsische IT-Planungsrat die Leitlinie zur Gewährleistung der Informationssicherheit (ISLL) beschlossen und in Kraft gesetzt (Nds. MBl. 2011, Seite 518). Sie verpflichtet die unmittelbare Landesverwaltung, ein wirkungsvolles Informationssicherheitsmanagementsystem (ISMS) aufzubauen sowie dauerhaft aufrechtzuerhalten und weiterzuentwickeln.

Die Sicherheitslage wird für die niedersächsische Landesverwaltung durch das beim Ministerium für Inneres und Sport bestehende Niedersachsen-CERT (Computer Emergency Response Team),

den Informationssicherheitsbeauftragten der Landesverwaltung (Chief Information Security Officer - CISO) und durch die Informationssicherheitsbeauftragten der Behörden ständig bewertet. Gegebenenfalls notwendige organisatorische und technische Maßnahmen werden in direkter Zusammenarbeit mit den IT-Dienstleistern in der niedersächsischen Landesverwaltung umgesetzt. Dabei werden die nach dem jeweiligen Stand der Technik angemessenen Schutzmechanismen angewendet, um Daten vor unberechtigtem Zugriff zu schützen.

In den Vergabeverfahren der niedersächsischen Landesverwaltung ist es gängige Praxis, dass von den Bietern auch die Anforderungen aus Sicht des Datenschutzes, des Geheimschutzes, der Informationssicherheit, der Notfallvorsorge und des vorbeugenden personellen Sabotageschutzes erfüllt werden müssen. Bei der Vergabe von IT-Leistungen werden die allgemein gültigen Bestimmungen des Vergaberechts auf nationaler und europäischer Ebene angewendet.

Dies vorausgeschickt, beantworte ich die Anfrage namens der Landesregierung wie folgt:

Zu 1:

Die Bemühungen der Bundesregierung, zum Schutz der inneren und äußeren Sicherheit sowie der staatlichen Souveränität den heimlichen Abfluss von Regierungswissen an fremde Mächte mit einer sogenannten No Spy Garantie und weiteren Regelungen zu verhindern, werden von der Landesregierung begrüßt.

In der Landesregierung wird die Möglichkeit einer Einführung vergleichbarer Regelungen in der niedersächsischen Landesverwaltung derzeit umfassend geprüft.

Zu 2:

Die Vergabe von IT-Leistungen erfolgt in der niedersächsischen Landesverwaltung auf Grundlage von Ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen (EVB-IT) gemäß § 55 Bundeshaushaltsordnung (BHO) und Beschlüssen des IT-Planungsrats Bund/Länder, die auch in Niedersachsen durch Runderlass verbindlich sind. Den EVB-IT werden Geheimhaltungsvereinbarungen und Leistungsbeschreibungen sowie gegebenenfalls zusätzliche Merkblätter (z. B. für Geheimschutz) beigefügt. Die Anforderungen aus Sicht des Datenschutzes, des Geheimschutzes, der Informationssicherheit, der Notfallvorsorge und des vorbeugenden personellen Sabotageschutzes sind wichtige Bestandteile der Leistungsverzeichnisse. Die Leistungsanforderungen an die Informationssicherheit, die Notfallvorsorge und den Datenschutz zum Vergabegegenstand werden insbesondere anhand der jeweils vorliegenden Vorabkontrollen nach § 7 Nds. Datenschutzgesetz in der gültigen Fassung, der Sicherheitskonzepte gemäß der Leitlinie zur Gewährleistung der Informationssicherheit (Nds. MBl. 2011, Seite 518) und der Notfallvorsorgekonzepte im Leistungsverzeichnis spezifiziert und anschließend zum Vertragsbestandteil gemacht. Die nationalen Standards des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik und die internationalen Standards (z. B. Internationale Zertifizierungsnorm für Informationssicherheitsmanagementsysteme - ISO 27001) werden insofern berücksichtigt. Daneben wird von den Bietern mit dem Angebot der Nachweis gefordert, dass die für die Umsetzung des Auftrags vorgesehenen Firmenmitarbeiter (sowie Mitarbeiter von Subunternehmern) die notwendige Eignung, Fachkunde und Erfahrung im Hinblick auf Informationssicherheit, Notfallvorsorge und Datenschutz besitzen. Im Falle des Einsatzes von Firmenmitarbeitern (bzw. Mitarbeitern von Subunternehmern) an sicherheitsempfindlichen Stellen (z. B. Wartungsarbeiten im Rechenzentrum) gelten die Regelungen des vorbeugenden personellen Sabotageschutzes i. d. F. vom 30.03.2004. Die Einforderung der Bereitschaft, dass sich Mitarbeiter der zu beauftragenden Firmen den Bedingungen des Nds. Sicherheitsüberprüfungsgesetzes (Nds. SÜG) zu unterwerfen und Verpflichtungserklärungen zur Informationssicherheit zu unterzeichnen haben, hat sich bewährt. Ferner sind bei bestimmten Vergaben die Vorgaben der Verschlusssachenanweisung für das Land Niedersachen i. d. F. vom 13.02.1997 mit ihren ergänzenden Richtlinien beim Einsatz von Informationstechnik zu beachten.

Im Übrigen verweise ich auf die Vorbemerkungen.

Zu 3:

Die Landesregierung prüft derzeit umfassend, ob bundesweit einheitliche Regelungen erforderlich sind, um ein Auseinanderdriften der vergaberechtlichen Anforderungen zur IT-Sicherheit in Bund und Ländern zu vermeiden und ein hohes gemeinsames Sicherheitsniveau zu erreichen. Vor die-

sem Hintergrund steht die Landesregierung in engem Austausch mit anderen Ländern und dem Bund.

Zu 4:

Die Daten der Landesverwaltung werden grundsätzlich auf behördeneigenen Servern oder Servern im Herrschaftsbereich des landeseigenen Dienstleisters IT.Niedersachsen gespeichert. Dabei werden die Daten auf magnetischen Speichermedien, weit überwiegend auf Festplatten in Servern oder speziellen Speichersystemen (Storagesysteme) gespeichert.

IT.Niedersachsen wird als Dienstleister im Rahmen der Auftragsdatenverarbeitung für andere Landesbehörden tätig und ergreift verschiedene Maßnahmen, um eine missbräuchliche Nutzung von Daten bei IT.Niedersachsen auszuschließen:

– IT.Niedersachsen betreibt ein eigenes Informationssicherheitsmanagementsystem (sogenanntes ISMS), welches in einem fortwährenden Prozess den Umgang mit Informationen vor dem Hintergrund der Gewährleistung der Vertraulichkeit, Verfügbarkeit und Integrität regelt und kontrolliert.

– Den Belangen der Informationssicherheit trägt IT.Niedersachsen entsprechend Nummer 7.1.2 der Leitlinie zur Gewährleistung der Informationssicherheit (ISLL/Nds. MBl. 2011, Seite 518) insbesondere durch einen hauptamtlichen Informationssicherheitsbeauftragten mit den Aufgaben gemäß Nummer 6.3.2 ISLL Rechnung. Dessen Tätigkeit wird durch den ebenfalls hauptamtlich bestellten behördlichen Datenschutzbeauftragten flankiert.

– Für jedes Verfahren bei IT.Niedersachsen werden die dem Stand der Technik entsprechenden angemessenen Sicherungsmaßnahmen anhand anerkannter Standards (z. B. IT-Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik, DIN/ISO 27001) ermittelt und umgesetzt.

– Neben einer Reihe von technischen Einzelmaßnahmen, welche von den jeweils eingesetzten IT-Infrastrukturkomponenten abhängen, legen z. B. Rechtekonzepte fest, wer Zugriff auf die in den Systemen verarbeiteten Daten haben darf und welche Arten der Verarbeitung im Einzelfall zulässig und folglich technisch möglich sind.

Die bei IT.Niedersachsen tätigen Landesbediensteten sind kraft Gesetzes dem Datengeheimnis gemäß § 5 des Niedersächsischen Datenschutzgesetzes (NDSG) verpflichtet. Bei der Möglichkeit des Zugangs zu sensiblen Systemen wird überdies eine Überprüfung nach dem Nds. SÜG durchgeführt. Auftragnehmer von IT.Niedersachsen werden vertraglich dazu verpflichtet, ihr Personal auf das Datengeheimnis zu verpflichten und auf die damit im Zusammenhang stehenden Strafvorschriften hinzuweisen. Vor dem ersten Einsatz wird Personal von Auftragnehmern durch IT.Niedersachsen nochmals belehrt. Auch im Zusammenhang mit Personal von Auftragnehmern werden beim Vorliegen der gesetzlichen Voraussetzungen Überprüfungen nach dem Nds. SÜG durchgeführt, soweit selbiges nicht bereits durch das Bundesministerium für Wirtschaft und Technologie geheimschutzbetreut ist. Schließlich gewährleistet § 6 NDSG die Einhaltung der Anforderungen aus dem NDSG durch IT.Niedersachsen im Verhältnis zu entsprechenden Auftragnehmern.

Hiervon abweichend werden in einigen Bereichen der Landesverwaltung Daten auf Servern von Kommunen einschließlich Dienstleistern in kommunaler Trägerschaft (z. B. HannIT, KDO), anderer Bundesländer oder des Bundes verarbeitet und/oder gespeichert. Vereinzelt werden Daten auch bei privaten IT-Dienstleistern und anderen Firmen im Rahmen von Auftragsdatenverarbeitungen verarbeitet und/oder gespeichert. Auch in diesen Fällen werden die nach innen und außen geltenden rechtlichen, technischen und organisatorischen Sicherheitsstandards und -techniken angewandt. Die Offenlegung detaillierter Angaben der Daten und Firmen in einer auch der Öffentlichkeit zugänglichen Beantwortung einer sogenannten Kleinen Anfrage unterbleibt an dieser Stelle aus Gründen des Wohls des Landes (Artikel 24 Abs. 3 NV), da die IT-Sicherheit des Landes Niedersachsen tangiert ist. Auf Wunsch wird die Landesregierung die Einzelheiten gern in einer vertraulichen Sitzung des zuständigen Fachausschusses mitteilen.

Verwaltungsdaten (Personal-, Studierenden-, Haushalts- und sonstige Daten der Hochschulverwaltung) der Hochschulen werden grundsätzlich nicht außerhalb des Hochschulbereiches gespeichert. Daten aus dem Bereich Lehre werden i. d. R. im Lernmanagementsystem Stud.IP auf Hochschul-

servern gespeichert. Forschungsdaten sollen grundsätzlich auf internen Servern gespeichert werden. Hierzu wurde an den niedersächsischen Hochschulen die hochschulübergreifende Hochschul-Storage-Cloud aufgebaut. Bei Forschungsverbundprojekten mit bundesweiter oder internationaler Beteiligung kann es erforderlich sein, dass Forschungsdaten außerhalb Niedersachsens gespeichert werden. Bei Forschungsprojekten mit Beteiligung oder auf Veranlassung von Wirtschaftsunternehmen kann es erforderlich sein, Forschungsdaten auch bei den beteiligten Firmen zu speichern. Bediensteten der Hochschulen ist die Nutzung von Onlinespeicherdiensten wie DropBox in der Regel über die Nutzungsordnung der Hochschulrechenzentren untersagt. Soweit Daten auf Servern oder Cloud-Strukturen im (gegebenenfalls deutschlandweiten) Hochschulbereich liegen, wird Datenmissbrauch u. a. durch technische Maßnahmen (grundlegende Rechtevergabe, Firewalls, Kryptotechnik, Zugriffsprotokollierung) und durch Zugangsregelungen über die Niedersächsische Hochschul-Authentifizierungs- und Autorisierungsinfrastruktur (Nds-AAI) oder die deutschlandweite DFN-AAI des Wissenschaftsnetzes verhindert.

Trotz der genannten umfassenden Maßnahmen liegt es in der Natur der Sache, dass es einen absoluten Schutz vor Datenmissbrauch nicht geben kann.

Boris Pistorius



(Ausgegeben am 15.12.2014)