

**Kleine Anfrage zur schriftlichen Beantwortung  
mit Antwort der Landesregierung**

Anfrage der Abgeordneten Christian Grascha, Björn Försterling und Jörg Bode (FDP)

Antwort des Niedersächsischen Finanzministeriums namens der Landesregierung

**Brandsätze im Finanzamt Hannover-Land I**

Anfrage der Abgeordneten Christian Grascha, Björn Försterling und Jörg Bode (FDP), eingegangen am 17.01.2018 - Drs. 18/206  
an die Staatskanzlei übersandt am 23.01.2018

Antwort des Niedersächsischen Finanzministeriums namens der Landesregierung vom 22.02.2018,  
gezeichnet

Reinhold Hilbers

**Vorbemerkung der Abgeordneten**

Das Finanzamt Hannover-Land I wurde in den letzten Wochen mehrfach Ziel von geplanten Brandanschlägen mit Brandsätzen. Insgesamt ist laut Medienberichten von drei Brandsätzen auszugehen, welche in jeweils unterschiedlichen Gebäudeteilen deponiert wurden. In einem ersten Fall vom 4. Dezember 2016 wurde der Brandsatz im Archiv, am 5. Januar 2017 in einem Aktenraum und am 6. Januar 2017 an einem aus ermittlungstaktischen Gründen nicht benannten Ort deponiert.

**Vorbemerkung der Landesregierung**

Die Bundesrepublik Deutschland ist ein freiheitlicher demokratischer Rechtsstaat, der einen gesetzeskonformen Umgang von Bürgern mit der öffentlichen Verwaltung und umgekehrt organisieren und garantieren muss. Dabei ist das angemessene Verhältnis von Bürgerfreundlichkeit einerseits und Verfahrenssicherheit andererseits von großer Bedeutung. Es muss immer wieder neu geprüft und durch geeignete Maßnahmen hergestellt werden. Der Austausch der öffentlichen Verwaltung mit Ratsuchenden und Leistungsberechtigten wird in öffentlichen Einrichtungen mitunter durch Konflikte belastet. In Ausnahmefällen sehen sich Bedienstete teilweise extremen Formen von Bedrohungen und Übergriffen ausgesetzt.

Das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) hat hierzu Sicherheitsinformationen erstellt, die für sämtliche Behörden mit Publikumsverkehr gelten. In der Handreichung „Gewalt am Arbeitsplatz. Beschäftigte vor Übergriffen schützen.“ werden verschiedene Maßnahmen vorgestellt, die helfen können, Kundenübergriffe am Arbeitsplatz zu reduzieren, die Intensität der Gewalt zu mindern und diese im besten Fall zu verhindern. Sie gibt überdies Ratschläge, wie die Gefahrensituation einzelner Arbeitsplätze eingeschätzt werden kann und welche Maßnahmen sich an den jeweiligen Arbeitsplätzen zur Vorbeugung von Übergriffen am besten eignen. Die Handreichung geht zurück auf die Broschüre der niedersächsischen Polizei „Sicherheit an Arbeitsplätzen mit Publikumsverkehr“, die im Jahr 2013 erstellt wurde.

Darüber hinaus wird angesichts der wachsenden Zahl von Angriffen auf Behördenmitarbeiterinnen und Behördenmitarbeiter durch das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) Informationsmaterial zur Optimierung der Sicherheit von Beschäftigten der öffentlichen Verwaltung gegen Gewalt am Arbeitsplatz zur Verfügung gestellt.

Ein entsprechendes Falblatt enthält ferner Hinweise, wie sich Bedienstete an ihren Arbeitsplätzen vor Übergriffen schützen können und was in einer Krisensituation und im Anschluss daran zu tun ist.

Seit Ende 2017 kann das Informationsmaterial u. a. von der Polizei bezogen werden; die Broschüren stehen auf den Internetseiten des ProPK zum Herunterladen zur Verfügung (<http://www.polizeiberatung.de/nc/startseite-und-aktionen/aktuelles/detailansicht/mehr-sicherheit-am-arbeitsplatz-1>).

Zusätzlich stehen die Ansprechpersonen für Kriminalprävention der Polizei Niedersachsen für themenbezogene Anfragen zur Verfügung.

Hinsichtlich des Einbaus und der Nutzung von Zutrittssicherungen und der sonstigen Sicherheitsvorkehrungen bei den Dienstgebäuden der Landesverwaltung sind unterschiedliche Ausgangslagen zu berücksichtigen. Entsprechend der Funktionalität des jeweiligen Dienstgebäudes und Grundstücks (Verwaltung, Labor, Gebäude mit Freiflächen) bedarf es nicht überall gleichermaßen umfangreicher und wirkungsvoller Sicherheitsvorkehrungen.

Durch die Einführung eines umfassenden Informationssicherheitsmanagementsystems (ISMS) hat die Landesregierung die Voraussetzungen für einen sicheren und datenschutzkonformen Umgang mit Informationen geschaffen. Darin werden Verfahren und Regeln beschrieben, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Je nach physischer Beschaffenheit der Datenbestände (Papierakte, digitaler Datenbestand) werden datenschutzrelevante Unterlagen unter Verschluss aufbewahrt. Dies geschieht bei Papierakten entweder in gesonderten Räumen mit gegebenenfalls abschließbaren Schränken, auf die nur befugte Mitarbeiterinnen und Mitarbeiter Zugriff haben, oder durch elektronische Zutrittskontrollanlagen, die es ermöglichen, Zugangsrechte zielgerichtet zu vergeben. Die Zugangsberechtigung zu digitalen Datenbeständen wird über Signaturkarten, personenbezogene Computer-ID, persönliche Passwörter und individuelle Zugriffsrechte auf den berechtigten Personenkreis eingeschränkt. Sofern eine Anbindung an das Landesnetz besteht, liegen die Daten auf gesicherten Servern des Landes oder - wie z. B. im Bereich der Steuerverwaltung - auf gesicherten Servern beim „Data Center Steuern“ in Rostock.

### **1. Wie stellt die Landesregierung in ihren Behörden die Sicherheit von Mitarbeitern und Bürgern sicher?**

Die Sicherheit von Bürgerinnen und Bürgern sowie Mitarbeiterinnen und Mitarbeitern wird in niedersächsischen Behörden durch etablierte und den lokalen Gegebenheiten und Anforderungen angepasste Maßnahmen (beispielsweise durch Zugangskontrollen, Ausstellung von Ausweisen/Dienstausweisen, Vorhalten technischer Sicherungseinrichtungen sowie Einsatz von Sicherheitsdiensten) gewährleistet.

### **2. Wie wird sichergestellt, dass nur Befugte Zutritt zu datenschutzrelevanten Unterlagen haben?**

Niedersächsische Staatskanzlei, Niedersächsisches Ministerium für Bundes- und Europaangelegenheiten und Regionale Entwicklung, Niedersächsisches Landesarchiv (StK und MB)

Datenschutzrelevante Unterlagen werden in den Diensträumen aufbewahrt und sind dort außerhalb der Arbeitszeiten unter Verschluss aufzubewahren, sodass nur befugte Bedienstete Zugang haben.

Niedersächsisches Ministerium für Inneres und Sport (MI)

Die Sicherung von datenschutzrelevanten Unterlagen erfolgt gemäß den rechtlichen Vorgaben.

Niedersächsisches Finanzministerium (MF)

Die Leitlinie zur Gewährleistung der Informationssicherheit beinhaltet den Aufbau eines Informationssicherheitsmanagements in der niedersächsischen Landesverwaltung.

Die Informationssicherheit umfasst alle organisatorischen, personellen und technischen Maßnahmen, die erforderlich sind, um Informationen (Daten, Dateien, Akten) zu schützen.

Mit der Bestellung des Informationssicherheitsbeauftragten für die Sicherheitsdomäne MF wurde das Informationssicherheitsmanagementsystem im MF installiert. Die Sicherheitsdomäne MF umfasst alle Arbeitsplätze in den Liegenschaften Schiffgraben 10, Blumenstr. 6, Theaterstr. 16 (4. OG), und alle in der Dienststelle vorhandenen Telearbeitsplätze.

Niedersächsisches Landesamt für Bezüge und Versorgung (NLBV)

Im NLBV werden datenschutzrelevante Unterlagen entsprechend der dortigen Datenschutzanweisung in verschlossenen Aktenräumen aufbewahrt, sodass nur berechnigte Personen Zugriff auf die Unterlagen haben.

Steuerverwaltung (LStN, Finanzämter)

Zur Realisierung einer homogenen Informationssicherheit im Bereich der Steuerverwaltung wird beim LStN ein „Informationssicherheitsmanagementsystem“ (ISMS) betrieben.

Im Rahmen dieses ISMS wurde speziell für den Einsatzbereich der Finanzämter ein Schutzzonenmodell entwickelt und in 2017 eingeführt. Im Rahmen dieses Modells werden die Schutzbedarfe für jedes einzelne Finanzamt ermittelt und geeignete Maßnahmen zur Erreichung, Einhaltung und Optimierung des entsprechenden Schutzbedarfs umgesetzt.

Staatliches Baumanagement (NLBL, Bauämter)

Zur Realisierung einer homogenen Informationssicherheit wird im Bereich der Bauverwaltung beim NLBL ein „Informationssicherheitssystem“ (ISMS) aufgebaut. Im Dezember 2016 wurden im Rahmen von Ortsbegehungen im Dienstgebäude Waterloostr. 4 alle sich im Gebäude befindlichen Schutzobjekte aufgenommen und der aktuelle Stand der Sicherheitsmaßnahmen festgestellt. Im Rahmen einer Arbeitsgruppe ISLL NLBL soll nunmehr für den Einsatzbereich ein Schutzzonenmodell entwickelt und für die Dienststellen des Staatlichen Baumanagements eingeführt werden. In diesem Zusammenhang werden geeignete Maßnahmen zur Erreichung, Einhaltung und Optimierung des entsprechenden Schutzbedarfs umgesetzt.

Niedersächsisches Ministerium für Soziales, Gesundheit und Gleichstellung (MS)

In den Dienststellen sind datenschutzrelevante Unterlagen vor unbefugter Einsicht zu schützen. Bei Abwesenheit oder nach Dienstschluss sind entsprechende Unterlagen in Aktenschränken einzuschließen. Zugriffsrechte auf datenschutzrelevante, digitale Daten sind durch persönliche Kennwörter und Sperrung der Arbeitsplätze beim Verlassen der Büroräume geschützt.

In einigen Dienststellen werden zusätzlich die Räume, in denen sich datenschutzrelevanten Unterlagen befinden, mit mechanischen oder elektronischen Schließsystemen gesichert.

Die Einrichtungen des Maßregelvollzugszentrums sind geschlossen.

Niedersächsisches Ministerium für Wissenschaft und Kultur (MWK)

Je nach physischer Beschaffenheit der Datenbestände (Papierakte, digitaler Datenbestand) werden datenschutzrelevante Unterlagen unter Verschluss aufbewahrt. Dies geschieht bei Papierakten entweder in gesonderten Räumen mit abschließbaren Stahlschränken, auf die nur befugte Mitarbeiterinnen und Mitarbeiter Zugriff haben. Teilweise sind elektronische Zutrittskontrollanlagen im Einsatz, die es ermöglichen, Zugangsrechte zielgerichtet zu vergeben. Die Zugangsberechtigung zu digitalen Datenbeständen wird über Signaturkarten, personenbezogene Computer-ID, persönliche Passwörter und individuelle Zugriffsrechte eingeschränkt. Sofern eine Anbindung an das Landesnetz besteht, liegen die Daten auf gesicherten Servern des Landes.

Niedersächsisches Kultusministerium (MK)

In der Sicherheitsdomäne MK, die auch den nachgeordneten Bereich umfasst, bestehen sowohl organisatorische als auch technische Regelungen der Zutritts- und Zugriffskontrolle zur Erhöhung der Informationssicherheit. Die organisatorischen Regelungen sind in den Anwenderanweisungen der einzelnen Behörden gemäß der ISLL und ISRL des Landes festgeschrieben. Dort wird sowohl der Zutritt zu als auch der Zugriff auf Daten des Landes umfassend geregelt. Unbefugten Personen ist der Zugriff auf diese Daten verwehrt.

Niedersächsisches Ministerium für Wirtschaft, Arbeit und Verkehr (MW)

Grundsätzlich können sich Unbefugte nicht ohne Begleitung Bediensteter in den Dienstgebäuden bewegen. Besonders sensible datenschutzrelevante Unterlagen werden in verschlossenen Räumen und Schränken aufbewahrt. Zugriff haben nur befugte Personen.

## Landesamt für Bergbau, Energie und Geologie (LBEG)

Alle Beschäftigten sind durch die Grundstücks- und Hausordnung angehalten, ihre Dienstzimmer, Labore und die anderen Räumlichkeiten, die zur Aufgabenerledigung genutzt werden (wie z. B. Rechnerräume, Besprechungsräume), jederzeit vor unbefugtem Eindringen zu sichern. Dafür existieren u. a. Schlüssel, die nach Verlassen der Dienststelle in gesicherten Schlüsselkästen aufbewahrt werden. Datenschutzrelevante Unterlagen werden in verschlossenen Schränken aufbewahrt.

## Niedersächsische Landesbehörde für Straßenbau und Verkehr (NLStBV)

Datenschutzrelevante Unterlagen werden in verschließbaren Schränken aufbewahrt. Diese stehen im unmittelbaren Sichtbereich der jeweiligen Sachbearbeitung. Auf dem Dienstweg werden Unterlagen mit diesbezüglichen Inhalten nur in verschlossenen Umlaufmappen versandt. Archivierte Unterlagen befinden sich in verschlossenen Kellern, deren Zugang nur ausgesuchtem Personal möglich ist.

## Landesbetrieb für Mess- und Eichwesen (MEN)

Für den Umgang mit Datenschutz und IT-Sicherheit im Innen- sowie Außendienst gibt es Dienst-anweisungen und Dienstvereinbarungen.

## Materialprüfanstalt (MPA) Braunschweig

Die Mitarbeiterinnen und Mitarbeiter sind angewiesen, keine Unterlagen in öffentlichen Bereichen dauerhaft oder vorübergehend zu lagern. Büros sind beim Verlassen abzuschließen. Arbeitsplatzrechner müssen gesperrt werden und können nur durch die Eingabe eines Passworts wieder entsperrt werden. Die Zugriffsberechtigungen für Datenbestände sind so gestaltet, dass nur Personen Zugriff haben, die damit innerhalb einer Arbeitsgruppe fachlich befasst sind.

## Materialprüfanstalt (MPA) Hannover

Zugriff haben nur Berechtigte mit entsprechenden Passwörtern und Schlüsselberechtigungen.

Niedersächsisches Ministerium für Ernährung, Landwirtschaft und Verbraucherschutz (ML)

Der Zutritt zu besonders zu schützenden Gebäudeteilen und Räumen, wo datenschutzrelevante Unterlagen abgelegt sind, ist durch besondere Schließungen oder Freischaltungen bei elektronisch verschlossenen Zugängen geregelt. Nur autorisierte Bedienstete haben Zugang. Soweit dies aus organisatorischen oder baulichen Gründen nicht angezeigt ist, werden diese Unterlagen in abschließbaren Metallschränken verwahrt.

Niedersächsisches Justizministerium (MJ)

Der Zutritt zu den Justizgebäuden einschließlich des Justizministeriums und die Absicherung von nichtöffentlichen Gebäudeteilen werden durch die jeweilige Behördenleitung individuell nach den örtlichen Bedürfnissen durch eine Hausordnung geregelt.

Hinsichtlich der IT-Sicherheit sind folgende Regelungen getroffen:

Sämtliche in der niedersächsischen Justiz eingesetzten IT-Geräte sind in der Regel durch ein Passwort gegen unberechtigten Zugang gesichert. Die Anwenderinnen und Anwender haben bei Verlassen des Arbeitsplatzes ihre IT-Geräte zu sperren, sodass ein erneuter Zugang nur mittels eines Passworts möglich ist.

Die auf den Datenträgern der Clientsysteme abgelegten Daten der Justiz werden zum einen lokal durch einen Behörden-Server und zum anderen zentral durch Justizserver (sogenannte HUB-Sites) gespeichert und damit vor unbefugtem Zugriff und Elementarschäden gesichert.

Der Zutritt und Gebrauch von Serverräumen wie auch von HUB-Sites-Rechnerräumen in der niedersächsischen Justiz unterliegt besonderen Regelungen, die in einer Dienstanweisung niedergelegt sind, deren Aktualität in regelmäßigen Abständen überprüft wird.

#### Niedersächsisches Ministerium für Umwelt, Energie, Bauen und Klimaschutz (MU)

Der Umgang mit datenschutzrelevanten Daten wird regelmäßig überprüft. Über die IT-Sicherheit und Zugangskonzepte wird sichergestellt, dass entsprechende Daten nur von berechtigten Personen verarbeitet werden können. In Papierform dürfen diese Daten ebenfalls nur von berechtigten Personen verarbeitet werden und müssen je nach Schutzstufe entsprechend sicher verwahrt werden. Über den Hauserlass zur Besucherregelung wird der Zugang zum Gebäude und damit auch zu möglichen Daten kontrolliert. Die Mitarbeiterinnen und Mitarbeiter sind angehalten, ihre Büroräume in Abwesenheit abzuschließen. Zu den Gefahren für schützenswerte Informationen am Arbeitsplatz wurden die Mitarbeiterinnen und Mitarbeiter des Hauses zudem in den vergangenen Jahren in mehreren Veranstaltungen zum Thema Informationssicherheit sensibilisiert

#### Gewerbeaufsichtsämter

In den Gewerbeaufsichtsämtern sind datenschutzrelevante Unterlagen vor unbefugter Einsicht zu schützen. Bei Abwesenheit oder nach Dienstschluss sind entsprechende Unterlagen einzuschließen. Arbeitsplatzrechner müssen gesperrt werden und können nur durch die Eingabe eines Passworts wieder entsperrt werden. Der Zutritt und Gebrauch von Serverräumen unterliegt besonderen Regelungen. Weitere Regelungen ergeben sich in den Staatlichen Gewerbeaufsichtsämtern durch die ISLL und eine sicherheitsdomänenspezifische Dienstanweisung zur Umsetzung der ISRL des Landes sowie durch Hausanweisungen und Dienstvereinbarungen. Für die Sicherheitsdomäne der Gewerbeaufsichtsämter wurde eine zentrale Informationssicherheitsbeauftragte bestellt. Zu den Gefahren für schützenswerte Informationen am Arbeitsplatz wurden die Mitarbeiterinnen und Mitarbeiter der Ämter zudem in den vergangenen Jahren in mehreren Veranstaltungen zum Thema Informationssicherheit sensibilisiert.

#### NLWKN

Die informationssicherheitstechnischen Rahmenbedingungen für die Bearbeitung von digitalen und analogen Daten werden im NLWKN durch IT-Sicherheitskonzepte und Informationssicherheitsrichtlinien in Form von Dienstanweisungen für den IT-Betrieb und die einzelnen Bearbeitungsprozesse geregelt.

In den vergangenen Jahren wurden Mitarbeiterinnen und Mitarbeiter durch persönliche Einweisungen, Informationsveranstaltungen sowie Informationen im Intranet und das Angebot von eLearnings mit Multiple Choice Tests in den Themen Informationssicherheit und Datenschutz bedarfsgerecht unterwiesen. Die Maßnahmen werden weiterhin laufend angeboten, insbesondere für neue Mitarbeiterinnen und Mitarbeiter.

Unterjährige Überprüfungen finden statt, in besonderen Fällen - z. B. der EU-Zahlstelle - auch durch externe Audits, hier durch das ML etc.

Daneben sind die Mitarbeiterinnen und Mitarbeiter mit Zugriff auf personenbezogene Daten verpflichtet, ihre Büroräume bei Verlassen abzuschließen. Personenbezogene Daten werden darüber hinaus in abschließbaren Schränken aufbewahrt, digitale personenbezogene Daten werden auf gesonderten Servern mit entsprechend gesicherten Zugriffsrechten vorgehalten.

Serverräume sind mit einer Zugangssicherung ausgestattet.

#### Alfred-Toepfer-Akademie für Naturschutz

Datenschutzrelevante Unterlagen werden in den Diensträumen aufbewahrt und sind dort außerhalb der Arbeitszeiten unter Verschluss aufzubewahren, sodass nur befugte Bedienstete Zugang haben.

#### Nationalparkverwaltung Harz

Datenschutzrelevante Unterlagen werden in den Diensträumen aufbewahrt und stehen dort außerhalb der Dienstzeiten unter Verschluss. Zugang haben somit nur Befugte. Der Zugang zu digitalen

Datenbeständen wird durch personenbezogene Computer-ID, persönliche Passwörter und individuelle Zugriffsrechte gesichert.

Nationalparkverwaltung Wattenmeer

Digitale Datenbestände sind nach den üblichen Vorgaben (personenbezogene Computer-ID, persönliche Passwörter, individuelle Zugriffsrechte) und im Landesnetz gesichert und stehen damit grundsätzlich nur den betreffenden Mitarbeiterinnen und Mitarbeitern zur Verfügung. Unterlagen in Papierform werden in den einzelnen Diensträumen aufbewahrt, die bei Abwesenheit des oder der jeweiligen Beschäftigten in der Regel abgeschlossen sind; im Übrigen sind die Diensträumlichkeiten insgesamt durch grundsätzlich verschlossene Türen gesichert. Außerhalb der Dienstzeiten sind zudem die Gebäudeaußentüren durch ein elektronisches Zugangssystem gesichert.

Biosphärenreservat Elbtalaue

Über die IT-Sicherheit und Zugangskonzepte wird beim Umgang mit datenschutzrelevanten Daten sichergestellt, dass entsprechende Daten nur von berechtigten Personen verarbeitet werden können. Besonders sensible datenschutzrelevante Unterlagen in Papierform werden in verschlossenen Schränken aufbewahrt, auf die nur befugte Personen Zugriff haben. Die Schränke stehen im unmittelbaren Sichtbereich der jeweiligen Sachbearbeitung.

**3. Wie konnte es in diesen drei konkreten Fällen geschehen, dass Unbefugte Zugang zu den o. g. Räumlichkeiten hatten?**

Diese Frage ist Gegenstand der laufenden polizeilichen Ermittlungen. Gesicherte Informationen hierzu liegen derzeit noch nicht vor. Die polizeilichen Ermittlungen werden jedoch mit Hochdruck vorangetrieben.

(Verteilt am 27.02.2018)