

Antwort auf eine Große Anfrage

- Drucksache 16/2270 -

Wortlaut der Großen Anfrage der Fraktion Bündnis 90/Die Grünen vom 04.03.2010

Wer speichert was, warum, wieso und wie lange, und an wen kann es weitergegeben werden?

Der Datenschutz hat nach dem Urteil des Bundesverfassungsgerichts zur Volkszählung von 1983 Grundrechtscharakter. Das Gericht forderte seinerzeit, dass die Bürgerinnen und Bürger wissen müssen, wo, was, wann, warum über sie gespeichert sei, da ansonsten das Vertrauen in Staat und Gesellschaft erheblich leide. Mit der Zunahme von neuen Speichertechnologien und Vernetzungssystemen haben Speicherdateien jeglicher Art in hohem Maße zugenommen. Das verfassungsrechtliche Gebot von Bestimmtheit und Transparenz staatlicher Dateien scheint dabei zu erodieren. Das Verwaltungsgericht Hannover hat am 22. Mai 2008 entschieden, dass für die Datei „Gewalttäter Sport“ in Niedersachsen die Rechtsgrundlage fehlt. Auch an der BKA-Datei „APIS“ gibt es erhebliche Kritik hinsichtlich der Rechtsklarheit und Eingriffstiefe.

Die ständige Ausweitung von Sammeldateien durch den Staat muss nach Auffassung von Beobachtern deutlich strenger hinterfragt und parlamentarisch kontrolliert werden. Es ist mittlerweile für die Bürgerinnen und Bürger kaum noch nachvollziehbar, wer, wie oft, wie lange und warum in welcher Datei gespeichert wird, welche notwendige Informationsgewinnung damit verbunden ist, welche Vorteile und Ermittlungserfolge für den Staat mit solchen Dateien verbunden sind und an wen die gespeicherten Daten weitergegeben werden können und dürfen. Die „Sammelleidenschaft“ des Staates zur Kontrolle und zum vermeintlichen Schutz seiner Bürgerinnen und Bürger wird ständig ausgeweitet. Das Bundesverfassungsgericht hat das Gesetz über die Vorratsdatenspeicherung in einer Entscheidung jüngst als verfassungswidrig eingestuft. Auch in Niedersachsen wurden in den letzten sechs Jahren verschiedene neue Dateien und Überwachungsinstrumente geschaffen. Die Datenschützer von Bund und Ländern sind daher besorgt.

Fragwürdig bei der neuen Sicherheitspolitik sind in den Augen von Sachverständigen vor allem der Ausbau sogenannter Vorfeldbefugnisse und die Überwachung von Kontakt- und Begleitpersonen. Damit vergrößert sich die Gefahr, dass auch unbescholtene und rechtstreue Bürger in den Fokus staatlicher Überwachung geraten. Und der Datenaustausch wird mittlerweile nicht nur zwischen verschiedenen Behörden eines Bundeslandes oder des Staates praktiziert, sondern hat globale Ausmaße angenommen. Jüngst hat es erhebliche Kritik am Fluggastdatenaustausch der Bundesrepublik mit den USA sowie am SWIFT-Abkommen gegeben.

Der Grundrechtsschutz durch Organisation und Verfahren müsse im Kontext von Informationsgewinnung eine entscheidende Rolle spielen, fordert das Bundesverfassungsgericht. Die tragenden Eckpfeiler des grundrechtlich verbürgten Datenschutzes sind das Erfordernis einer hinreichend bestimmten gesetzlichen Grundlage, die Zweckbindung, die Verhältnismäßigkeit sowie die Möglichkeit der Rechtsmäßigkeitkontrolle. Dennoch heißt es im Grundlagenwerk von Lisken/Denninger „Handbuch des Polizeirechts“: „Für den Bürger geht der klare Maßstab verloren, unter welchen Voraussetzungen er mit der Speicherung seiner Daten bei der Polizei rechnen muss.“ Und an anderer Stelle: „In dem Gewirr polizeilicher Dateien ist ein Überblick kaum noch möglich.“

Wir fragen die Landesregierung:

1. Welche grundsätzlichen Aufgaben und Ziele haben folgende Dateien oder Datenbanken?
 - a) NIVADIS
 - b) POLAS
 - c) APIS

*) Die Anlagen sind im Intranet und im Internet einsehbar.

- d) PIOS
 - e) INPOL
 - f) KAN
 - g) APS
 - h) Castortransporte - ISAS
 - i) SAFIR
 - j) SAFIR-Castor
 - k) LKA-System Castor
 - l) LIMO
 - m) REMO
 - n) AUMO
 - o) Gewalttäter Sport
 - p) GIAZ Niedersachsen
 - q) Anti-Terror-Datei
 - r) ZEVIS
2. Um was für konkrete Dateien/Datenbanken aus der Frage 1 handelt es sich jeweils, d. h.:
- a) Handelt es sich um eine niedersächsische, bundesweite, europäische oder internationale Datei, Datenbank, Projektdatei o. Ä.?
 - b) Handelt es sich um eine Volltext- oder Index-Datei?
 - c) Wer wird aufgrund welches Tatvorwurfs/Deliktes, Vorfalls oder sonstiger Voraussetzung darin gespeichert?
 - d) Welche Informationen werden gespeichert?
 - e) Wie lange werden die Personen und Informationen gespeichert?
 - f) Wie viele Personen sind darin gespeichert?
 - g) Wer hat Zugriff auf die vollständigen Dateien oder auf einen Teilbereich, und wovon hängt der vollständige oder teilweise Zugriff ab?
 - h) Wo bzw. bei wem werden sie zentral gespeichert?
 - i) Wann werden die Daten in den Dateien gelöscht?
 - h) Aufgrund welcher Rechtsgrundlage wurden die Dateien geschaffen und betrieben?
 - k) Welche Rechtsschutzmittel haben die betroffenen Bürgerinnen und Bürger gegen die Speicherungsmaßnahme?
 - l) Welche konkreten Auswirkungen hat eine Speicherung für die betroffene Person (Hintergrund: Eintrag in „Gewalttäterdatei Sport“ führt zu einem dreijährigen bundesweiten Stadionverbot, selbst wenn vor Gericht ein Freispruch erfolgt)?
3. Auf welche niedersächsischen, bundesweiten, europäischen oder internationalen Dateien, Datenbanken, Projektdateien o. Ä. haben die niedersächsische Polizei und der niedersächsische Verfassungsschutz zusätzlich zu den in der Frage 1 genannten Dateien Zugriff? Bitte die Dateien konkret bezeichnen.
4. Um was für Dateien/Datenbanken handelt es sich jeweils bei den zu Frage 3 genannten, d. h.:
- a) Welches Ziel haben die einzelnen Dateien?
 - b) Wer wird aufgrund welches Tatvorwurfs/Deliktes, Vorfalls oder sonstiger Voraussetzung darin gespeichert?
 - c) Welche Informationen werden gespeichert?

- d) Wie lange werden die Personen gespeichert?
 - e) Wer hat Zugriff auf die vollständigen Dateien oder auf einen Teilbereich, und wovon hängt der vollständige oder teilweise Zugriff ab?
 - f) Wo bzw. bei wem werden sie zentral gespeichert?
 - g) Wann werden die Daten in den Dateien gelöscht?
 - h) Aufgrund welcher konkreten Rechtsgrundlage wurden die Dateien geschaffen und betrieben?
 - i) Wie viele Personen sind darin gespeichert?
 - j) Aufgrund welcher Rechtsgrundlage wurden die Dateien geschaffen und betrieben?
 - k) Welche Rechtsschutzmittel haben die betroffenen Bürgerinnen und Bürger gegen die Speicherungsmaßnahme?
 - l) Welche konkreten Auswirkungen hat eine Speicherung für die betroffene Person?
5. In welchen der Dateien sind Abgeordnete des Niedersächsischen Landtages, des Deutschen Bundestages oder des Europäischen Parlaments gespeichert:
 - a) In welchen Dateien sind Personen eingespeichert worden, die zum Zeitpunkt der Speicherung Mitglied eines der genannten Parlamente waren (bitte auflisten nach Jahreszahl der Speicherung, Parlament und Fraktion)?
 - b) In welchen Dateien sind Personen eingespeichert worden, die später Mitglied eines der genannten Parlamente geworden sind (bitte auflisten nach Jahreszahl der Speicherung, Parlament und Fraktion)?
 - c) Wie viele Mitglieder der genannten Parlamente sind gegenwärtig in welcher der Dateien gespeichert (bitte auflisten nach Parlament und Fraktion)?
 6. Gibt es einen systematischen Überblick (Gesamtverfahrensverzeichnis) oder eine Metadatenbank, auf wie viele Dateien und Datenbanken die niedersächsischen Sicherheitsbehörden (Polizei, Justiz, Verfassungsschutz) insgesamt zugreifen können?
 7. Wenn ja, um wie viele Dateien und Datenbanken handelt es sich dabei insgesamt?
 8. Bei welchen Dateien haben Betroffene die Möglichkeit abzufragen, welche Informationen über sie gespeichert werden?
 9. In welchen Dateien, Verbunddateien, Projektdateien des Bundes und/oder der Länder wurden z. B. die eingekesselten Personen anlässlich des Castortransports in Pudripp am 10. November 2006 gespeichert?
 10. Welche Möglichkeiten haben Bürgerinnen und Bürger hinsichtlich der Kontrolle und Löschung ihrer erfassten und gespeicherten Daten, wenn diese an andere Staaten, EU und Nicht-EU-Mitglieder weitergegeben werden?
 11. An welche niedersächsische oder bundesdeutsche Behörde müssen sich Bürgerinnen und Bürger wenden, um in Erfahrung zu bringen, an welche zuständige Behörde sie sich im Drittstaat wenden müssen, um Informationen über ihren Datenbestand zu bekommen, wenn der Drittstaat personenbezogene Daten aus Deutschland erhalten hat?
 12. Wie viele Fälle von rechtlich unzulässigen Speicherungen von Daten von Personen hat es in den letzten fünf Jahren in Niedersachsen gegeben?
 13. Sind bei unrechtmäßiger Datenspeicherung den betroffenen Personen durch die Speicherung Nachteile entstanden? Wenn ja, welche, und wie wurden sie entschädigt?
 14. Wie werden die gesetzlich vorgeschriebenen Löschrümpflichten von staatlichen Datensätzen kontrolliert und umgesetzt?

15. Kommt es nach § 486 STPO in Verbindung mit § 20 des Justizmitteilungsgesetzes zu einer definitiven Mitteilung an die Polizei, wie das erkennende Gericht einen Strafprozess entschieden hat?
16. Wie verhindert die Landesregierung, dass es zu rechtlich unzulässigen Verdachtsspeicherungen kommt, also Personen weiterhin in elektronischen oder anderweitigen Kriminalakten geführt werden, obwohl das gerichtliche Verfahren keine Verurteilung nach sich gezogen hat?
17. Werden bei der computergestützten Übermittlung von personenbezogenen Daten zwischen Behörden stets Verschlüsselungstechniken angewendet?
18. Welche technischen Prinzipien und Sicherungen der Zugangskontrolle zu staatlichen Datenbanken werden in Niedersachsen praktiziert?
19. Welche technischen Sicherungen gegen unbefugtes Kopieren und Verwenden von Datenbanken mit personenbezogenen Datensätzen werden in Niedersachsen praktiziert?
20. Welche weiteren Dateien und Datenbanken zur Speicherung persönlichkeitsrelevanter Merkmale plant die Landesregierung in dieser Legislatur?
21. Ist stets gewährleistet, dass bei einer weiteren Einrichtung einer Datei/Datenbank die niedersächsische Datenschutzbehörde einbezogen wird?
22. Ist stets gewährleistet, dass bei einer weiteren Einrichtung einer Datei/Datenbank der gerichtliche Rechtsschutz für betroffene Personen offensteht?

Antwort der Landesregierung

Niedersächsisches Ministerium
für Inneres und Sport

Hannover, den 25.08.2010

Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil vom 15. Dezember 1983 die Grundlagen des modernen Datenschutzrechts gelegt. Die rasante Entwicklung im Bereich der Informationstechnologie und ihre Ausbreitung im privaten ebenso wie im öffentlichen Bereich hat in den fast 27 Jahren seit Erlass des Urteils jedoch neue Möglichkeiten und Gefahren gebracht und Veränderungen in den Rechtsgrundlagen für die Datenverarbeitung erforderlich gemacht. Technische Neuerungen wie das Internet und der Mobilfunk beeinflussen unser Arbeiten, die Kommunikation, die Freizeitgestaltung, das Lernen, Spielen sowie den Konsum in erheblicher und nachhaltiger Weise. Diese Veränderungen führen auch zu neuen Formen kriminellen Handelns - im Rahmen der Alltagskriminalität genauso wie im Bereich der organisierten Kriminalität.

Zu diesen gesellschaftlichen und technischen Veränderungen tritt eine grundlegend geänderte allgemeine Gefahrenlage hinzu, wie sie sich in den Anschlägen in den USA vom 11. September 2001 manifestiert hat. Zahlreiche weitere Anschläge und Anschlagversuche in den letzten Jahren zeigen, dass auch Europa und damit Deutschland im Fadenkreuz des internationalen Terrorismus steht.

Diese Entwicklungen mussten auch die Arbeit der niedersächsischen Sicherheitsbehörden¹ verändern. Sie haben neue Anforderungen an ihre Tätigkeit gestellt, aber auch neue Möglichkeiten und Instrumente der Analyse und des Handelns geschaffen. Namentlich zur Bekämpfung des internationalen Terrorismus sind zielgerichtete Informationen und ein effektiver Datenaustausch auch über Staatsgrenzen hinweg unabdingbar. Damit gewinnt die internationale Zusammenarbeit, vor allem auch innerhalb der Europäischen Union als Raum der Freiheit, der Sicherheit und des Rechts, eine immer größere Bedeutung.

¹ Unter Hinweis der genannten Geschäftsbereiche in der Frage 6 dieser Anfrage erfolgt eine Beantwortung für die Landespolizei, den niedersächsischen Verfassungsschutz sowie für die niedersächsische Justiz, die sich im Folgenden als niedersächsische Sicherheitsbehörden verstehen.

Die Gewährleistung der Sicherheit der Bürgerinnen und Bürger ist eine Kernaufgabe des Staates. Die Bevölkerung erwartet einen handlungsfähigen Staat, der die notwendigen Maßnahmen ergreift, um Gefahren rechtzeitig zu identifizieren und zu bekämpfen. Ebenso notwendig ist eine wirksame Strafrechtspflege. Zur Erfüllung dieser Aufgaben ist eine moderne Datenverarbeitung unverzichtbar.

Die wirksame Bekämpfung von Kriminalität und Terrorismus und der Datenschutz als Ausdruck des Grundrechts auf informationelle Selbstbestimmung stellen keine unüberbrückbaren Gegensätze dar. Das Bundesverfassungsgericht hat nach dem grundlegenden Volkszählungsurteil gerade in jüngster Zeit eine Reihe von wegweisenden Entscheidungen zum Datenschutz getroffen, insbesondere zur akustischen Wohnraumüberwachung, Telekommunikationsüberwachung, Rasterfahndung, Online-Durchsuchung und zur sogenannten Vorratsdatenspeicherung. Wesentliche Voraussetzungen der Verfassungsmäßigkeit von Eingriffsgrundlagen sind nach diesen Entscheidungen des Bundesverfassungsgerichts ein hinreichend bestimmter und verhältnismäßiger Eingriffstatbestand, der den Anlass von Datenerhebungen und den Kreis der Betroffenen determiniert, Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung, Vorkehrungen zum Grundrechtsschutz durch Verfahren und bei verdeckten Datenerhebungen auch die Gewährleistung nachträglichen Rechtsschutzes.

Das Niedersächsische Gesetz über die öffentliche Sicherheit und Ordnung (Nds. SOG) wurde mit Gesetz vom 25. November 2007 im Bereich der polizeilichen Datenerhebung überarbeitet, um den Vorgaben des Bundesverfassungsgerichts Rechnung zu tragen. In diesem Zusammenhang wurde auch der Begriff der Kontakt- und Begleitpersonen neu definiert und enger gefasst. Damit ist klargestellt, dass die Verbindung zur Verdachtsperson eine bestimmte Qualität aufweisen und mit der angenommenen Straftat in einem Zusammenhang stehen muss. Insgesamt sind die sogenannten Vorfeldbefugnisse, die der Polizei nach dem Nds. SOG zur Verhütung von Straftaten zustehen, so ausgestaltet, dass sie nur bei einer bestimmten Verdachtslage ausgeübt werden können, die je nach Art des Eingriffs unterschiedlich ausgeprägt sein muss.

Die Rechtsgrundlagen der Datenverarbeitung und des Datenschutzes, die sich für den Bereich der Sicherheitsbehörden im Wesentlichen aus dem Nds. SOG, dem Nds. Verfassungsschutzgesetz (NVerfSchG), dem Nds. Datenschutzgesetz (NDSG) sowie aus dem Bundeskriminalamtgesetz (BKAG) und der Strafprozessordnung (StPO) ergeben, werden den verfassungsrechtlichen Anforderung in vollem Umfang gerecht. Eine ins Einzelne gehende Regelung polizeilicher Dateien ist auf gesetzlicher Ebene naturgemäß aufgrund der Vielgestaltigkeit und Unvorhersehbarkeit polizeilicher Aufgabenwahrnehmung nicht möglich. Das Bestimmtheitsgebot verlangt aber, dass in abstrakt-genereller Weise die Voraussetzungen für die Datenspeicherung und Übermittlung geregelt werden und für die Bürger erkennbar ist, welche Behörden in welchem Sachzusammenhang Daten über sie verarbeiten dürfen.

Die auf den Regelungen des BKAG basierende Datei „Gewalttäter Sport“ hat das Bundesverwaltungsgericht mit Urteil vom 9. Juni 2010 für rechtmäßig erklärt, nachdem die im BKAG vorgesehene Rechtsverordnung durch das Bundesministerium des Innern erlassen worden war.

Die Umsetzung des Rechts erfolgt in der Zielsetzung einer effektiven und effizienten staatlichen Verwaltung. Dafür berücksichtigen auch die niedersächsischen Sicherheitsbehörden kontinuierlich technische und rechtliche Entwicklungen, um ihre Mittel zur Aufgabenerfüllung an die sich ändernden Bedingungen anzupassen. So stellt z. B. der Einsatz von computergestützten Vorgangsbearbeitungssystemen ebenso wie die Einrichtung von zweckgebundenen Dateien und Anwendungen² ein unverzichtbares Instrument der modernen und intelligenten Aufgabenerfüllung dar. Dabei gehen die niedersächsischen Sicherheitsbehörden mit den personenbezogenen Daten ihrer Bürgerinnen und Bürger verantwortungsbewusst um.

² Dateien (Dateien, Datenbanken und Projektdaten) und Anwendungen im Sinne der Anfrage sind solche, in denen personenbezogene Daten verarbeitet werden. Davon ausgenommen sind allgemein zugängliche Dateien und Anwendungen, bzw. solche, in denen lediglich personenbezogene Daten von Mitarbeiterinnen und Mitarbeitern der niedersächsischen Sicherheitsbehörden verarbeitet werden.

Die niedersächsischen Sicherheitsbehörden haben zur Erfüllung ihrer jeweiligen Aufgaben eigene Dateien und Anwendungen eingerichtet und können auf sogenannte Verbunddateien, internationale Dateien und Anwendungen zurückgreifen. Die hohe Anzahl der vorhandenen Dateien resultiert keineswegs nur aus der Notwendigkeit einer effektiven Kriminalitätsbekämpfung und Strafverfolgung. Sie ist nicht zuletzt auch im Datenschutz selbst begründet, denn sie begrenzt die jeweiligen Anwenderkreise. Beispielsweise stehen sensible Opferdaten genauso wie alle weiteren gespeicherten Inhalte in einer Datei nur den zur betreffenden Aufgabenerfüllung vorgesehenen Stellen zur Verfügung. Des Weiteren trägt die Trennung von Dateien der grundsätzlichen Trennung zwischen Justiz, Verfassungsschutz und Polizei Rechnung.

Die Beantwortung der Großen Anfrage erfolgt auf Grundlage der Zulieferungen durch die beteiligten Bundesministerien bzw. -behörden. Hinsichtlich der Beantwortung der Anzahl der in Anwendungen gespeicherten Personen (Fragen 2 f bzw. 4 i) erfolgte eine Erhebung mit Stand April 2010.

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

Zu 1:

Spezifische Angaben zu Aufgaben und Zielen der Dateien und Anwendungen sind den genannten Anlagen zu entnehmen.

- a) **NIVADIS** - Landesanwendung „Niedersächsisches Vorgangsbearbeitungs-, Analyse-, Dokumentations- und Informations-System“ (**Anlage 1**, dazu **Anlage 1 a**)
- b) **POLAS** - Landesanwendung „Polizeiliches Auskunftssystem“ (**Anlage 2**)
- c) **APIS**³ - jetzt Verbunddatei „Innere Sicherheit“ (**Anlage 3**)
- d) **PIOS**⁴ - jetzt Verbunddatei „Arbeitsdatei PIOS (Personen, Institutionen, Objekte, Sachen) Organisierte Kriminalität APOK“ (**Anlage 4**)
- e) **INPOL** - Informationssystem, das sich aus den Anwendungen „Personenfahndung“, „Haftdatei“, „KAN“ und „Erkennungsdienst“ zusammensetzt. (**Anlage 5**)
- f) **KAN** - Kriminalaktennachweis - Siehe Antwort zu 1 e)
- g) **APS** - Landesanwendung „Auswertungsprogramm Polizeilicher Staatsschutz“ (**Anlage 6**)
- h) **Castortransporte - ISAS** - jetzt Landesanwendung „Castortransporte - ISA (Informations-, Sammel- und Auswertestelle)“ (**Anlage 7**)
- i) **Safir** - Landesanwendung „Software zur Analyse, Fallbearbeitung, Informationsverarbeitung und Recherche“ (**Anlage 8**)
- j) **Safir-Castor** - Landesanwendung zur anlassbezogenen Abwicklung des Castortransportes (**Anlage 9**)
- k) **LKA-System Castor** - Dieses System ist den niedersächsischen Sicherheitsbehörden nicht bekannt.
- l) **LIMO** - Bei der Bezeichnung handelt es sich nicht um eine Datei oder Anwendung, sondern um einen personengebundenen Hinweis „Straftäter, politisch links orientiert“ innerhalb des Informationssystems Inpol. (siehe **Anlage 5**)
- m) **REMO** - Die Bezeichnung stellt einen personengebundenen Hinweis „Straftäter, politisch rechts motiviert“ dar. Siehe auch Antwort zu Frage 1 l).
- n) **AUMO** - Die Bezeichnung steht für den personengebundenen Hinweis „Straftäter, politisch motivierter Ausländerkriminalität“ im Inpol. Siehe auch Antwort zu Frage 1 l).

³ Aus Gründen der Vereinfachung sowie der potenziell vorhandenen Verwechslungsgefahr mit ehemaligen Dateien PIOS (siehe auch Beantwortung zu Frage 1 d) wurde die „Arbeitsdatei PIOS - Innere Sicherheit“ in „Innere Sicherheit“ umbenannt.

⁴ Die Datei PIOS für Organisierte Kriminalität wurde in APOK umbenannt (siehe auch Beantwortung zu Frage 1c).

- o) **Gewalttäter Sport** - Verbunddatei (**Anlage 10**)
- p) **GIAZ Niedersachsen** - Landesanwendung „Gemeinsames Informations- und Analysezentrum Polizei und Verfassungsschutz“ (**Anlage 11**)
- q) **Anti-Terror-Datei** - Bundesdatei „ATD“ auf Grundlage des Antiterrordateigesetzes (**Anlage 12**)
- r) **ZEVIS** - „Zentrales Verkehrsinformationssystem“ (**Anlage 13**)

Im Übrigen siehe Vorbemerkungen.

Zu 2:

Die Beantwortungen der Fragestellungen zu 2 a bis 2 j⁵ sind den jeweils zu Frage 1 a bis 1 r genannten Anlagen zu entnehmen. Die Beantwortungen zu Frage 2 d stellen eine abschließende Übersicht dar, welche Inhalte innerhalb der jeweiligen Datei oder Anwendung gespeichert werden dürfen. Die tatsächlich abgelegten Inhalte richten sich stets nach den Erfordernissen des Einzelfalles.

- k) Je nach Rechtsgrundlage der Datei bestehen für die betroffenen Bürgerinnen und Bürger folgende Rechtsschutzmöglichkeiten gegen Speicherungsmaßnahmen:

Betroffene können bezüglich ihrer gespeicherten personenbezogenen Daten Ansprüche geltend machen auf Berichtigung nach § 17 Abs. 1 NDSG, auf Löschung nach § 39 a Nds. SOG, § 17 Abs. 2 Nr. 1 NDSG und auf Sperrung nach § 39 a Nds. SOG, § 17 Abs. 3 NDSG. Nach § 17 a NDSG besteht ein Widerspruchsrecht gegen die Verarbeitung entsprechender Daten. Kenntnis von den über sie gespeicherten Daten können Betroffene über ihr Auskunfts- und Akteneinsichtsrecht nach § 16 NDSG erlangen.

Bei verdeckten Datenerhebungen ist durch entsprechende Unterrichtungspflichten sicher gestellt, dass Betroffenen Kenntnis von gegen sie gerichtete Maßnahmen erhalten und ihre Rechte geltend machen können.

Speichermaßnahmen auf der Grundlage des BKAG richten sich nach den dort enthaltenen bereichsspezifischen Regelungen, wobei hier das BDSG ergänzend zur Anwendung kommt. Anträge auf Berichtigung, Löschung und Sperrung sind nach § 32 BKAG zu stellen. Sie sind an das BKA zu richten, soweit sie eine Amtsdatei des BKA betreffen. Bei Verbunddateien des polizeilichen Informationssystems Inpol nach § 11 BKAG müssen sich die Betroffenen gemäß § 32 Abs. 9 BKAG an die verantwortliche Stelle wenden, also an die Daten eingebende Polizeibehörde des Bundes bzw. des Landes.

Bei Verbunddateien gilt § 19 BDSG in Verbindung mit § 12 Abs. 5 BKAG, das heißt, die Auskunft wird durch das BKA nur im Einvernehmen mit der verantwortlichen Polizeibehörde des Bundes oder des Landes erteilt.

Bei erfolglosen Anträgen gegenüber den verantwortlichen Stellen steht den Betroffenen der Verwaltungsgerichtsweg offen.

Hinsichtlich der Anwendungen ZEVIS und AZR wird auf die entsprechenden **Anlagen 13 und 25** verwiesen.

- l) Eine Speicherung einer Person in einer Datei oder Anwendung der niedersächsischen Sicherheitsbehörden hat zum Zeitpunkt der Speicherung keine unmittelbare Auswirkung auf den Betroffenen zur Folge.

So führt ein Eintrag in die Datei „Gewalttäter Sport“ zu keinem Stadionverbot, vielmehr kann ein Stadionverbot zu einem Eintrag in die Datei „Gewalttäter Sport“ führen.

⁵ Da die Ziffer h) im Rahmen der Fragestellung der Großen Anfrage zu Frage 2 zweimal vergeben wurde, wird die Frage „Aufgrund welcher Rechtsgrundlage wurden die Dateien geschaffen und betrieben?“ im Rahmen der Beantwortung im Folgenden als Ziffer 2 j) dargestellt.

Zuständig für das Aussprechen von Stadionverboten sind gemäß § 2 der Richtlinien zur einheitlichen Behandlung von Stadionverboten allein die originären Hausrechtsinhaber (Verein, DFB oder Ligaverband). Das Stadionverbot ist demnach keine staatliche Sanktion auf ein strafrechtlich relevantes Verhalten, sondern eine Präventivmaßnahme auf zivilrechtlicher Basis.

Zu 3:

Auf folgende niedersächsische⁶ Dateien und Anwendungen hat die niedersächsische Polizei Zugriff:

- **DAMASKUS** „Datei zur Massenauswertung von Kraftfahrzeugkennzeichen und sonstigen Daten“ (**Anlage 14**)
- **Dolmetscherdatei** (**Anlage 15**)
- **Einwohnermeldeamt-Abgleich** (**Anlage 16**)
- **ISI** „Intranet der Landespolizei Niedersachsen“ (**Anlage 18**)
- **OnlineWache** Internetanwendung zur webbasierten Anzeigeerstattung ohne eigenständige Datenspeicherung. Die eingegebenen Daten werden über die Anwendung EPOST 810 der zuständigen Polizeidienststelle übermittelt. Dort erfolgt eine manuelle Erfassung im Vorgangsbearbeitungssystem NIVADIS (**Anlage 19**).
- **Sterbedatenabgleich** (**Anlage 20**)
- **Themenbezogene Sammlungen (TBS)** - In NIVADIS integrierte Datenbankanwendungen, die als ermittlungsbegleitende Anwendungen, für spezielle Analysen bzw. Auswertungen zu unterschiedlichen, polizeilich relevanten Phänomenbereichen, genutzt werden. (**Anlage 21**)
 - TBS K.U.R.S. „Konzeption zum Umgang mit rückfallgefährdeten Straftätern“,
 - TBS Wasserschutzpolizei Seeschiffkontrollen,
 - TBS Fahrradbesitzerdatei Niedersachsen,
 - TBS Milieu Menschenhandel/Rotlichtmilieu.
- **Vorgangserfassung und -verwaltung Vermögensermittlungsverfahren im Land Niedersachsen** (**Anlage 22**)

Auf folgende bundesweite Dateien und Anwendungen hat die niedersächsische Polizei Zugriff:

- **AFIS-P** - Verbunddatei „Automatisiertes Fingerabdruck-System-Polizei“ (**Anlage 23**)
- **Auswertung RG** - Inpol-Falldatei „Rauschgiftkriminalität“ (**Anlage 24**)
- **AZR** - Anwendung des BVA „Ausländerzentralregister“ (**Anlage 25**)
- **DEO** - Inpol-Falldatei Dokumentation - Europa - Ost (**Anlage 26**)
- **DNA-Analysedatei** - Verbunddatei (**Anlage 27**)
- **DOMESCH** - Inpol-Falldatei „Dokumente/Menschenhandel/Schleusung“ (**Anlage 28**)
- **EPOST 810** polizeiliches Nachrichtenübertragungssystem (**Anlage 17**)
- **Falschgeld** - Inpol-Falldatei (**Anlage 29**)
- **FUZ** - Inpol-Falldatei „Fälschung unbarer Zahlungsmittel“ (**Anlage 30**)
- **FBK Waffen** - Falldatei Bundeskriminalamt (**Anlage 31**)
- **FBK Falschgeld** - Falldatei Bundeskriminalamt (**Anlage 32**)
- **FBK GER** - Falldatei Bundeskriminalamt „Geiselnahme/Erpressung/Raub“ (**Anlage 33**)
- **FBK Tötungs- und Sexualdelikte** - Falldatei Bundeskriminalamt (**Anlage 34**)

⁶ Niedersächsisch sind die Dateien und Anwendungen, die landesweit elektronisch abgefragt werden können.

- **FDR** - Verbunddatei „Falldatei Rauschgift“ (Anlage 35)
- **Datenbank für digitalisierte Finger- und Handflächenabdrücke - P** - Bundesdatei (Anlage 36)
- **Datenbank für digitalisierte Fingerabdrücke - A** - Verbunddatei (Anlage 37)
- **FUSION** Inpol-Falldatei „Rockerkriminalität“ (Anlage 38)
- **Gewalttäter links** - Verbunddatei (Anlage 39)
- **Gewalttäter Personenschutz** - Verbunddatei (Anlage 40)
- **Gewalttäter politisch motivierter Ausländerkriminalität** - Verbunddatei (Anlage 41)
- **Gewalttäter rechts** - Verbunddatei (Anlage 42)
- **IuK** - Verbunddatei „Informations- und Kommunikationskriminalität“ (Anlage 43)
- **Kinderpornografie** - Inpol-Falldatei (Anlage 44)
- **Korruption** - Inpol-Falldatei (Anlage 45)
- **NNSachKunst** - Verbunddatei „Nicht Numerische Sachfahndung Kunst“ (Anlage 46)
- **NSIS-Personenfahndung** - Verbunddatei „Nationales Schengener Informationssystem - Personenfahndung“ (Anlage 47)
- **NSIS-Sachfahndung** - Verbunddatei „Nationales Schengener Informationssystem - Sachfahndung“ (Anlage 48)
- **Sachfahndung** - Verbunddatei (Anlage 49)
- **SÄM-ÜT** - Inpol-Falldatei „Straftaten gegen ältere Menschen - überörtliche Täter“ (Anlage 50)
- **Schiffskontrolldatei** - bundesweite Datei (Anlage 51)
- **Solum Star/Solum Web** - Bundesanwendung - Zugriff besteht nur für den niedersächsischen Teil des Datenbestandes - (Anlage 52)
- **USA** - bundesweite Strafverfahrensdatei „Verdacht der Mitgliedschaft in einer terroristischen Vereinigung in Tateinheit mit Mord und Angriff auf den Luftverkehr“ (Anlage 53)
- **VEMAGS** - bundesweite Anwendung „Verfahrensmanagement für Großraum- und Schwertransporte“ (Anlage 54)
- **VERMI_UTOT** - Inpol-Falldatei „Vermisste/unbekannte Tote“ (Anlage 55)
- **ViCLAS** - Bundesanwendung „Violent Crime Linkage Analysis System/Analyse-System zur Verknüpfung von Gewaltverbrechen“ (Anlage 56)
- **WIKRI** - Inpol-Falldatei „Wirtschaftskriminalität“ (Anlage 57)

Auf folgende europäische bzw. internationale Dateien und Anwendungen hat die niedersächsische Polizei Zugriff:

- **ASF** - Interpol-Anwendung „Automated Search Facility/Automatisierte Suchfunktion“ (Anlage 58)
- **EUCARIS** - Europäische Anwendung „European Car and Driving License Information System/Europäisches Fahrzeug- und Führerschein- Informationssystem“ (Anlage 59)
- **EIS** - Europol-Anwendung „Europol-Informationssystem“ (Anlage 60)

Auf folgende niedersächsische Dateien und Anwendungen hat der niedersächsische Verfassungsschutz Zugriff:

- **Amtsdatei** - Landesdatei (Anlage 61)
- **G 10** - Landesdatei (Anlage 62)

Auf folgende bundesweite Dateien und Anwendungen hat der niedersächsische Verfassungsschutz Zugriff:

- **BLB** - Bundesdatei „Bundeslagebilddatei islamistischer Terrorismus“ (**Anlage 63**)
- **GBL** - Bundesdatei „Gewaltbereite Linksextremisten“ (**Anlage 64**)
- **Mujahedin Datei** - Bundesdatei (**Anlage 65**)
- **NADIS** - Bundesdatei „Nachrichtendienstliches Informationssystem“ (**Anlage 66**)

Zu 4:

Die Beantwortungen der Fragestellungen zu 4 a) bis 4 j) sind den zur Beantwortung der Frage 3 genannten Anlagen zu entnehmen. Die Beantwortungen zu Frage 4 c) stellen eine abschließende Übersicht dar, welche Inhalte innerhalb der jeweiligen Datei oder Anwendung gespeichert werden dürfen. Die tatsächlich abgelegten Inhalte richten sich stets nach den Erfordernissen des Einzelfalles.

k) Siehe Beantwortung zu Frage 2 k).

l) Siehe Beantwortung zu Frage 2 l).

Zu 5:

Die niedersächsischen Sicherheitsbehörden erfassen bzw. speichern Abgeordnete in keinen speziellen Dateien oder Anwendungen. Parlamentarier des Niedersächsischen Landtags, des Deutschen Bundestags oder des Europäischen Parlaments werden in Dateien, auf die die niedersächsischen Sicherheitsbehörden Zugriff haben, anlassbezogen - wenn die rechtlichen Voraussetzungen für eine Speicherung vorliegen - wie jede andere natürliche Person gespeichert. Eine strukturierte Erfassung ihrer parlamentarischen Zugehörigkeit erfolgt dabei jedoch nicht, sodass sich die Abgeordneten der verschiedenen Parlamente auch nicht gesondert herausfiltern lassen. Eine Ermittlung der Gesamtzahl von gespeicherten Angehörigen dieser Parlamente wäre für jede einzelne der 66 Dateien bzw. Anwendungen der niedersächsischen Sicherheitsbehörden durchzuführen. Für alle circa 1 500 Parlamentarier der aktuellen Wahlperioden würde dies 99 000 einzelne Abrufe erforderlich machen. Soweit zur Beantwortung der in die Vergangenheit zielenden Frage 5 a) und b) auch zurückliegende Wahlperioden in das Abrufverfahren einbezogen werden müssen, würden sich die Zahl der Parlamentarier und die Anzahl der einzelnen Abrufe nochmals erheblich potenzieren. Ein solches Verfahren ist mit einem außerordentlichen personellen Aufwand für die niedersächsischen Sicherheitsbehörden verbunden sowie mit erheblichen Eingriffen in die Rechte der Betroffenen. Aus Verhältnismäßigkeits- und Rechtsgründen wurde daher von einer Ermittlung aller nachgefragten Zahlen abgesehen.

Im Übrigen stehen Abgeordneten dieselben Auskunftsrechte wie jedem anderen Betroffenen zu. Siehe dazu Beantwortung zu Frage 8.

Für die Verbunddatei NADIS (**Anlage 66**) sind die nachfolgenden Angaben über Speicherungen von Parlamentariern in Dateien, bekannt:

- Für die Beantwortung von zwei Kleinen Anfragen im Deutschen Bundestag hat das Bundesamt für Verfassungsschutz (BfV) einmalig einen Abgleich der Daten aller Abgeordneter des Deutschen Bundestages seit der 1. Wahlperiode bis zur 16. Wahlperiode mit dem vorhandenen NADIS-Bestand durchgeführt. Das Ergebnis ist in der Beantwortung der zwei Kleinen Anfragen der Fraktion Bündnis 90/Die Grünen veröffentlicht (Sammlung, Speicherung und Weitergabe von Informationen über Bundestagsabgeordnete durch Geheimdienste - Drucksache 16/14159 und Erhebung, Speicherung und Weitergabe von Informationen über Bundestagsabgeordnete durch Geheimdienste in den Wahlperioden 1 bis 16 - Drucksache 16/14160).
- In der Antwort der Bundesregierung zu Frage 3 einer Kleinen Anfrage der Fraktion Bündnis 90/Die Grünen (Erhebung, Speicherung und Weitergabe von Informationen über Bundestagsabgeordnete durch Geheimdienste - Nachfragen zu Antworten der Bundesregierung auf entsprechende Kleine Anfragen der Fraktion Bündnis 90/Die Grünen - Drucksache 17/372) wurde mit Zustimmung der meisten Landesbehörden für Verfassungsschutz die aktuelle (Zeitpunkt

Dezember 2009) Anzahl der von ihnen im NADIS gespeicherten Abgeordneten des 17. Deutschen Bundestages veröffentlicht.

- Die Speicherungen im NADIS sind nicht statisch, sondern unterliegen einer stetigen Überprüfung. Der Niedersächsische Gesetzgeber hat die Verfassungsschutzbehörde in § 10 Abs. 2 Nr. 2 NVerfSchG verpflichtet, gespeicherte personenbezogene Daten zu löschen, wenn ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Die Erforderlichkeit der Daten ist bei der Einzelfallbearbeitung und nach festgesetzten Fristen (§ 10 Abs. 3 NVerfSchG) zu prüfen. Diese stetige Überprüfung durch die Niedersächsische Verfassungsschutzbehörde führt dazu, dass die Zahl der von ihr veranlassten Speicherungen im NADIS schwankend ist, sodass die Ende Dezember 2009 für die Beantwortung der o. a. Kleinen Anfrage (Drucksache 17/372) durch das BfV für Niedersachsen ermittelte Zahl gegebenenfalls nicht mehr aktuell ist. Insofern wurden die Zahlen der von Niedersachsen in NADIS durchgeführten Speicherungen von Abgeordneten des Deutschen Bundestages, des Europäischen Parlaments und des Niedersächsischen Landtags mit Hilfe des BfV aktualisiert bzw. wie folgt festgestellt:
 - 5 Speicherungen von Bundestagsabgeordneten,
 - 1 Speicherung einer Abgeordneten/eines Abgeordneten des Europäischen Parlaments und
 - 9 Speicherungen von Abgeordneten des Niedersächsischen Landtages.

Zum Schutz der Daten der Abgeordneten wird auf die angefragte Benennung der Fraktionszugehörigkeit verzichtet.

Von dieser zahlenmäßigen Auflistung sind Speicherungen aufgrund von Sicherheitsüberprüfungen bzw. Zuverlässigkeitsüberprüfungen ausgenommen. Bei diesen Speicherungen handelt es sich nicht um Speicherungen, die aufgrund einer Teilnahme an extremistischen Bestrebungen oder sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten vorgenommen werden. Vielmehr liegen diesen Speicherungen Sicherheitsüberprüfungen zugrunde, die z. B. bei den Mitgliedern der G 10-Kommission des Landes nach § 3 Abs. 2 Niedersächsisches Gesetz zur Ausführung des Artikel 10-Gesetzes durchgeführt werden, oder es handelt sich um Speicherungen aufgrund von Zuverlässigkeitsüberprüfungen z. B. nach dem Luftsicherheitsgesetz.

Diese Sicherheits- und Zuverlässigkeitsüberprüfungen werden nur mit Einverständnis der betroffenen Person in die Datenerhebung und die Speicherung der Daten durchgeführt.

Die Speicherungen personenbezogener Daten, die im NADIS vorgenommen werden, finden sich auch in der Amtsdatei (**Anlage 61**) der Niedersächsischen Verfassungsschutzbehörde, so dass auch in dieser Datei die o. a. aktuellen Speicherungen vorhanden sind.

Zu 6:

Ein Gesamtverfahrensverzeichnis oder eine Metadatenbank, auf wie viele Dateien und Datenbanken die niedersächsischen Sicherheitsbehörden (Polizei, Justiz, Verfassungsschutz) insgesamt zugreifen können, gibt es nicht.

Im Übrigen wird auf die Vorbemerkungen, Seite 3, verwiesen.

Zu 7:

Siehe Beantwortung zu Frage 6.

Zu 8:

Das Auskunftsrecht des Betroffenen richtet sich nach den jeweiligen Rechtsnormen, die in dem Bereich, für den Auskunft begehrt wird, gelten. Ob die Voraussetzungen dieser Normen im Einzelnen jeweils vorliegen, hat die zuständige Stelle zu prüfen.

Greifen keine spezialgesetzlichen Normen, ist dem Betroffenen gemäß § 16 NDSG von der Daten verarbeitenden Stelle auf Antrag Auskunft zu erteilen über die zu ihrer Person gespeicherten Daten. Außerdem sind insbesondere der Zweck und die Rechtsgrundlage der Speicherung sowie die Herkunft der Daten und die Empfänger von Übermittlungen mitzuteilen einschließlich der Auftragnehmer bei einer Auftragsdatenverarbeitung. Auskunftersuchen können abgelehnt werden, wenn

sonst die Aufgabenerfüllung der Daten verarbeitenden Stelle gefährdet würde, durch die Auskunftserteilung die öffentliche Sicherheit gefährdet oder dem Bund oder einem Land Nachteile bereiten würden oder die Daten nach einer Rechtsvorschrift oder aufgrund berechtigter Interessen Dritter geheim zu halten sind.

Zu 9:

Die personenbezogenen Daten der beteiligten Personen, die im Zusammenhang mit der Blockade des Castor-Transports im November 2006 bei Pudripp erhoben worden sind, wurden im Niedersächsischen Vorgangsbearbeitungssystem NIVADIS gespeichert. Darüber hinaus erfolgten Speicherungen personenbezogener Daten Betroffener in der Datenbank Castortransporte ISA, in der Landesanwendung APS und im Informationssystem Inpol. Soweit bei beteiligten Personen Ermittlungsverfahren eingeleitet worden sind, sind personenbezogene Daten im Geschäftsbereich der Justiz in der Verfahrensdatei web.sta bei der zuständigen Staatsanwaltschaft gespeichert.

Im Übrigen wird auf die Beantwortung der Kleinen Anfrage des Abgeordneten Prof. Dr. Hans-Albert Lennartz (GRÜNE) „Einschränkungen der Bürgerrechte beim Castortransport 2006“ durch die niedersächsische Landesregierung⁷ hingewiesen.

Zu 10:

Ansprüche auf Auskunft und Löschung in Bezug auf im Ausland gespeicherte Daten richten sich nach dem dort geltenden Recht. Eine Datenübermittlung ins Ausland darf nach den einschlägigen Bestimmungen - insbesondere § 43 Abs. 2 Nds. SOG, § 14 BKAG - nicht erfolgen, wenn in dem Empfängerstaat kein angemessenes Datenschutzniveau besteht.

Für die Mitgliedsstaaten der EU gilt der Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, der bis zum 27. November 2010 umzusetzen ist. Damit erfolgt eine Angleichung der datenschutzrechtlichen Regelungen in den Mitgliedsstaaten.

Für den Bereich des Niedersächsischen Verfassungsschutzes ist festgelegt, dass der Informationsaustausch mit ausländischen öffentlichen Stellen grundsätzlich dem BfV obliegt. Die Übermittlung personenbezogener Daten durch die niedersächsische Verfassungsschutzbehörde an Behörden ausländischer Staaten darf nur im Einvernehmen mit dem BfV und nur unter den engen Voraussetzungen des § 17 Abs. 3 des NVerfSchG erfolgen. Gemäß § 13 Abs. 1 Satz 2 NVerfSchG erteilt die niedersächsische Verfassungsschutzbehörde den betroffenen Bürgerinnen und Bürgern keine Auskunft über die Empfänger von übermittelten Daten. Die betroffenen Bürgerinnen und Bürger können sich im Rahmen eines Auskunftersuchens an den Landesbeauftragten für Datenschutz wenden (§ 13 Abs. 3 Satz 4 NVerfSchG).

Für den Geschäftsbereich der Justiz können Daten aus dem BZR im Rahmen des europäischen Registerverbundes NJR (Network of Judicial Registers) an die Partnerstaaten weitergegeben werden. Da die für die Datenverarbeitung verantwortliche Stelle über eine Weitergabe von Daten entscheidet, wäre eine Anfrage an das BZR zu richten. Es ist weder bekannt noch feststellbar, ob Auskünfte, die aus Datensätzen von Registereinträgen niedersächsischer Staatsanwaltschaften und Gerichte stammen, an Partnerstaaten des europäischen Registerverbundes weitergegeben worden sind.

Zu 11:

Bürgerinnen und Bürger können sich im Rahmen der ihnen zustehenden Auskunftsrechte nach § 16 NDSG, § 19 BDSG an die verantwortliche Stelle, das heißt, an die Daten erhebende Behörde wenden. Diese ist nach den genannten Rechtsvorschriften verpflichtet, auf Antrag auch Auskunft über die Empfänger von Übermittlungen ihrer personenbezogenen Daten zu geben.

Für den Bereich des Niedersächsischen Verfassungsschutzes wird auf die Beantwortung zu Frage 10 verwiesen.

⁷ Drucksache 15/3870 vom 08.06.2007

Für die niedersächsischen Justizbehörden wäre eine Anfrage an die registerführende Behörde zu richten. Bei Auskünften im Rahmen des europäischen Registerverbundes wäre die Anfrage beispielsweise an das BZR führende Bundesamt für Justiz zu richten.

Zu 12:

Nach Mitteilungen der niedersächsischen Polizeibehörden hat es in den letzten fünf Jahren insgesamt 87 Fälle von unzulässigen Datenspeicherungen gegeben.

Beim niedersächsischen Verfassungsschutz hat es keinen Fall von unzulässiger Datenspeicherung gegeben.

Im Geschäftsbereich der Justiz werden rechtlich unzulässige Speicherungen von Daten von Personen in den Statistiken nicht erfasst.

Ermittlungsverfahren im Zusammenhang mit dem Vorwurf rechtlich unzulässiger Speicherung von Daten in staatlichen Datenbanken sind von niedersächsischen Staatsanwaltschaften nicht geführt worden.

Zu 13:

Nach Mitteilung der Polizeibehörden werden derzeit in einem Fall Schadensersatzforderungen wegen einer unzulässigen Datenspeicherung vor dem Verwaltungsgericht geltend gemacht.

Für den niedersächsischen Verfassungsschutz wird auf die Beantwortung zu Frage 12 verwiesen.

Für den Bereich der Justiz sind keine Fälle bekannt, in denen Personen durch die Speicherung Nachteile entstanden sind.

Zu 14:

Mit der Speicherung eines personenbezogenen Datums in einer Datei bzw. Anwendung wird auf Basis der gesetzlichen Grundlagen dafür eine Prüffrist vergeben. Für jedes personenbezogene Datum erfolgt eine technische Darstellung des anstehenden Prüfauftrages. Die eigentliche Prüfung ist dann durch vorgeschriebene Abläufe in den betroffenen Geschäftsbereichen sichergestellt.

Sind personenbezogene Daten mit dem Einverständnis von Personen in Dateien und Anwendungen gespeichert, so sind diese auf Widerruf zu löschen.

Zu 15:

Nach § 482 Abs. 2, Satz 1 StPO unterrichtet die Staatsanwaltschaft die Polizeibehörde, die mit der Angelegenheit befasst war, über den Ausgang des Verfahrens durch Mitteilung der Entscheidungsformel, der entscheidenden Stelle sowie des Datums und der Art der Entscheidung. Die Übersendung eines Abdrucks der Mitteilung zum Bundeszentralregister ist zulässig, im Fall des Erforderns auch des Urteils oder einer mit Gründen versehenen Einstellungsentscheidung (§ 482 Abs. 2, Satz 2 StPO).

Zu 16:

Unter den Voraussetzungen der §§ 39 Abs. 3 Nds. SOG, 8 Abs. 3 BKAG, 484 Abs. 2 StPO dürfen Daten von Beschuldigten auch dann zur Verhütung und Vorsorge für die Verfolgung von Straftaten gespeichert werden, wenn das Strafverfahren nicht zu einer Verurteilung geführt hat.

Zu 17:

Durch das LSKN werden die Netze der niedersächsischen Polizei, des niedersächsischen Verfassungsschutzes sowie der Justizbehörden untereinander sowie gegenüber den Teilnetzen der anderen Landesbehörden getrennt. Innerhalb dieser separaten Datennetze werden Anwendungsverschlüsselungen für Datenübermittlungen eingesetzt.

Bei der Verarbeitung von Daten im Verbund mit anderen Sicherheitsbehörden in der Bundesrepublik Deutschland wird zusätzlich eine Leitungsverschlüsselung zum Schutz von Daten verwendet.

Zu 18:

Die niedersächsische Polizei betreibt ihre Datenbanken auf Basis des IT-Grundschutzes des BSI. Der Zugriff auf Daten einer Datei oder Anwendung setzt eine erfolgreiche Authentifizierung eines Anwenders durch Benutzername und Passwort voraus. Ein Zugriff auf physikalische Speichermedien ist ausschließlich den zuständigen Administratoren nach einer Authentifizierung und darüber hinaus in der Regel nur von dafür vorgesehenen Rechnern möglich.

Zugang zu den Räumlichkeiten, in den physikalische Speichermedien mit Daten aufgestellt bzw. aufbewahrt werden, haben nur besonders authentifizierten Mitarbeitern. Der kontrollierte Zugang wird durch technische Vorkehrungen sichergestellt.

Zutrittsmöglichkeiten zu Servereinheiten sowie Zugriff auf Datenbanken von Dateien und Anwendungen bestehen grundsätzlich nur für Server- und Datenbankadministratoren des LSKN, sowie die für die Datei oder Anwendung zuständigen Administratoren der ZPD. Ein Zugang für diese Mitarbeiter erfolgt über die Zugehörigkeit in definierten sowie zentral administrierten Berechtigungsgruppen, in denen Berechtigungsadministration und Anwendungsadministration personell voneinander getrennt sind.

Für den Bereich des niedersächsischen Verfassungsschutzes sind alle Rechner mit einem Passwortschutz versehen. Das Passwort wird bei einer Nichtbedienung des Rechners von mehr als zwei Minuten erneut abgefragt. Die Zugriffe werden entsprechend protokolliert.

Die Dateien, auf die der niedersächsische Verfassungsschutz zugreift, sind mit einem Zugriffskontrollsystem ausgestattet, mit dem der Zugriff auf Dateien durch besondere technische Verfahren auf den zugelassenen Benutzerkreis beschränkt wird.

Das Dienstgrundstück der niedersächsischen Verfassungsschutzbehörde stellt gemäß § 6 Abs. 5 Nds. SÜG einen Sicherheitsbereich dar, dessen Zugang mittels eines Kartensystems kontrolliert wird. Der Bereich der Wache ist auch zur Nachtzeit personell besetzt. Das Gebäude ist mit einer Alarmsicherung versehen, in denen besonders sicherheitsrelevante Räume (z. B. das Rechenzentrum) zusätzlich gesichert sind.

Im Geschäftsbereich der Justiz ist ein Zugang zu Dateien und Anwendungen nur über die jeweiligen Fachverfahren möglich. Die dort über alle Personen- und Verfahrensdaten vollständig implementierte Berechtigungssteuerung gewährt eine wirksame Zugangskontrolle. Die Mitarbeiter der Staatsanwaltschaften haben keine unmittelbare Datenbankberechtigung in den Datenbanken. Eine Datenbankberechtigung steht nur wenigen Systemadministratoren innerhalb des ZIB zu.

Zu 19:

Die niedersächsische Polizei betreibt Datenbanken mit personenbezogenen Daten auf Basis des IT-Grundschutzes gemäß BSI. Um unbefugtes Kopieren an NIVADIS-Arbeitsplätzen der Polizei zu verhindern, wurden die Rechner speziell konfiguriert. Ein Verwenden externer Datenträger, z. B. eines USB-Sticks oder einer externen Festplatte ist nicht möglich.

Eine Zugriffsberechtigung für die niedersächsischen Datenbanken des Verfassungsschutzes ist auf Systemadministratoren beschränkt. Die EDV-Betriebsstelle ist als speziell gesicherter Bereich mit einer Zugangskontrolle versehen, die ein unberechtigtes Betreten verhindert.

An den einzelnen Rechner-Arbeitsplätzen sind keine Datenexporte auf externe Datenträger möglich, da die Rechnerschnittstellen dauerhaft inaktiv geschaltet wurden.

Für den Bereich der Justiz wird auf die Beantwortung zu Frage 18 verwiesen.

Zu 20:

Die Landesregierung plant in dieser Legislaturperiode für den Bereich der niedersächsischen Sicherheitsbehörden zurzeit folgende Dateien bzw. Datenbanken zur Speicherung personenbezogener Daten:

Geschäftsbereich des MI:

a) Die Polizei sieht die

- Bereitstellung der Kriminalakten in elektronischer Form für berechnigte Mitarbeiter,
- Schaffung eines Personenregisters gemäß § 73 AufenthG sowie § 7 LuftSiG zur gesetzlichen Nachberichtsspflicht,
- Schaffung einer Archivierungsmöglichkeit nach den gesetzlichen Vorgaben des Niedersächsischen Archivgesetzes für elektronische Vorgänge aus NIVADIS,

vor.

b) Für den Bereich des Verfassungsschutzes wurde im Rahmen eines Bund-Länderbeschlusses eine Modernisierung für das Verbundsystem NADIS beschlossen. Mit dem NADIS WN (WissensNetz) soll die Grundlage für eine verbesserte Zusammenarbeit der Verfassungsschutzbehörden geschaffen und der Grundstein für Analysen der im Verfassungsschutz vorliegenden Informationen - insbesondere zu terroristischen Netzwerken - gelegt werden.

Ferner ist die Errichtung einer gemeinsamen Internet-Datenbank des Bundes und der Länder im Bereich Islamismus/islamistischer Terrorismus gemäß § 6 BVerfSchG vorgesehen.

Geschäftsbereich des MJ:

Im Rahmen des Projekts „Unterstützung von Umfangsverfahren“ ist geplant, die elektronische Doppelakte und die elektronische Handakte zu speichern.

In Planung ist ferner eine weitere Datenbank für ZIBOK. Die Daten aus dem BASIS-Web-Master sollen in einem Data Warehouse bereitgestellt werden. Dort sollen sie im Hinblick auf die Identifikation von Aktivitäten, die der organisierten Kriminalität zuzuordnen sind, ausgewertet werden. Die Speicherung zusätzlicher Daten wäre damit nicht verbunden.

Zu 21:

Eine Beteiligung des LfD⁸ Niedersachsen erfolgt gemäß § 22 Abs. 5 NDSG bei Einrichtung oder Änderung der Verfahren zur automatisierten Verarbeitung personenbezogener Daten auf Grundlage des NVerfSchG oder des Nds. SOG durch Übersendung der Beschreibungen gemäß § 8 NDSG.

Zu 22:

Ja.

Im Übrigen siehe auch Beantwortung zu Frage 2 k).

⁸ Im Sinne der Großen Anfrage werden der LfD sowie seine Mitarbeiter der Geschäftsstelle als „niedersächsische Datenschutzbehörde“ interpretiert.