

19. Wahlperiode

Schriftliche Anfrage

der Abgeordneten Gollaleh Ahmadi und June Tomiak (GRÜNE)

vom 30. Januar 2024 (Eingang beim Abgeordnetenhaus am 31. Januar 2024)

zum Thema:

Datenschutz beim Berliner Verfassungsschutz

und **Antwort** vom 9. Februar 2024 (Eingang beim Abgeordnetenhaus am 19. Februar 2024)

Frau Abgeordnete Gollaleh Ahmadi und Frau Abgeordnete June Tomiak (GRÜNE)
über
die Präsidentin des Abgeordnetenhauses

über Senatskanzlei – G Sen –

A n t w o r t

auf die Schriftliche Anfrage Nr. S19/18089
vom 30. Januar 2024
über Datenschutz beim Berliner Verfassungsschutz

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

1. Auf welche Datenbanksysteme haben Mitarbeiter*innen des Berliner Verfassungsschutzes Zugriff und inwiefern existieren eigene Datenbanken für den Berliner Verfassungsschutz?

Zu 1.:

Der Berliner Verfassungsschutz führt im Rahmen seines gesetzlichen Beobachtungsauftrages eine eigene Datenbank für die Registratur von Schriftgut. Daneben erfolgt eine dateimäßige Unterstützung einzelner Verwaltungstätigkeiten wie der Mitwirkung an Sicherheitsüberprüfungen und anderen gesetzlich vorgeschriebenen Überprüfungen. Durch Bundesrecht ist er verpflichtet, die folgenden gemeinsamen Dateien zu führen (Rechtsgrundlagen in Klammern):

- Nachrichtendienstliches Informationssystem des Verfassungsschutzverbundes (§ 6 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz)
- Antiterrordatei (§§ 1, 5 des Gesetzes zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern)
- Datei zur Bekämpfung des gewaltbezogenen Rechtsextremismus (§§ 1, 5 des Gesetzes zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden

und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus)

Zudem besteht Zugriff auf folgende Register, die der Berliner Verfassungsschutz im Wege automatisierter Abrufverfahren nutzt:

- Melderegister (§ 34 Bundesmeldegesetz)
- Gewerbedateien (§ 14 Abs. 11 iVm Abs. 6 der Gewerbeordnung)
- Gemeinsames Registerportal der Länder (§ 9 des Handelsgesetzbuches, jeweils iVm § 156 des Gesetzes betreffend die Erwerbs- und Wirtschaftsgenossenschaften und § 5 Abs. 2 des Gesetzes über Partnergesellschaften Angehöriger freier Berufe, § 79 des Bürgerlichen Gesetzbuches)
- Zentrales Fahrzeugregister (§ 36 Abs. 2 Satz 1 Nr. 3 iVm § 35 Abs. a Nr. 5 des Straßenverkehrsgesetzes)
- Ausländerzentralregister und Visadatei (§ 22 Abs. 1 Satz 1 Nr. 9 iVm § 20 Abs. 1 und § 32 Abs. 1 Nr. 8 und § 33 des Gesetzes über das Ausländerzentralregister)
- Nationales Waffenregister (§ 13 Nr. 8 iVm § 20 des Gesetzes zur Errichtung eines Nationalen Waffenregisters)

2. Inwiefern ist der Zugriff auf diese Datenbanksysteme auch über mobile Geräte möglich, welche Geräte und Betriebssysteme umfasst dies? Ist der Zugriff über mobile Endgeräte durch alle Mitarbeitenden des Landesamts möglich?

Zu 2.:

Aus Gründen des Geheimschutzes ist kein Zugriff über mobile Geräte möglich.

3. Wie wird sichergestellt, dass es weder bei festen Arbeitsplätzen noch mobilen Anwendungen Zugriff auf die Datensysteme durch unbefugte Dritte kommen kann, z.B. über eine Authentifizierung, Zugangskontrollen o.ä.?

4. Inwiefern werden Zugriffe auf Datenbanken über mobile Anwendungen und feste Arbeitsplätze durch Bedienstete des Landesamts für Verfassungsschutz erfasst bzw. kontrolliert und inwiefern und durch wen wird dies ausgewertet? Inwiefern lässt sich auf diesem Wege feststellen, ob unbefugte Dritte Zugriff auf die Datenbanken bekommen haben? (Falls solche Daten vorliegen, bitte nach Jahren seit 2018, Art des Zugriffs (mobil oder fester Arbeitsplatz) und Gegenstand der Abfrage aufschlüsseln)

5. Inwiefern wurden seit 2018 mobile Endgeräte mit Zugang zu solchen Datenbanken als Verlust gemeldet? Wie wird sichergestellt, dass unbefugte Dritte auch bei Verlust des mobilen Gerätes keinen Zugriff auf NADIS oder andere Datensysteme haben?

Zu 3. bis 5.:

Der Zugriff auf die Datenbanksysteme erfolgt ausschließlich über Arbeitsplätze innerhalb des mit entsprechenden Sicherheitsvorkehrungen versehenen Geheimschutzbereiches. Ein Zugriff durch unbefugte Dritte ist dadurch ausgeschlossen. Die Zugriffsberechtigung der

Mitarbeitenden sowie der Umfang der Zugriffsberechtigung wird geprüft und in Abhängigkeit des jeweiligen Aufgabenbereiches der Dienstkräfte personenscharf vergeben. Die Prüfung der Berechtigung erfolgt über ein automatisiertes Zugriffskontrollsystem mittels Benutzeridentifikation und Passwort. Alle Zugriffe werden protokolliert und revisionssicher aufbewahrt.

6. Welche (personenbezogenen) Daten werden in diesen Datenbanken erfasst? (bitte nach Kategorien aufschlüsseln)

Zu 6.:

Im Nachrichtendienstlichen Informationssystem des Verfassungsschutzverbundes werden ausschließlich die zur gesetzlichen Aufgabenerfüllung erforderlichen personenbezogenen Daten erfasst. Es handelt sich insbesondere um Daten, die zur Identifizierung der betroffenen Person erforderlich sind. Dazu zählen personenbezogene Grunddaten, wie zum Beispiel Name, Anschrift und Geburtsdatum. Weitergehende Angaben können aus Rechtsgründen nicht im Rahmen einer Schriftlichen Anfrage erfolgen. Eine detaillierte Darlegung, welche personenbezogenen Daten durch den Berliner Verfassungsschutz sowie den Verfassungsschutzverbund erfasst werden, würde Inhalte des Datenmodells offenlegen und unmittelbare Rückschlüsse auf die Arbeitsweise und die Fähigkeiten des Berliner Verfassungsschutzes sowie des Verfassungsschutzverbundes insgesamt zulassen. Der Anspruch auf Beantwortung der Schriftlichen Anfrage wird insoweit durch die Belange des Staatswohls begrenzt, um Gefahren für die Sicherheit des Landes Berlin sowie des Bundes und der übrigen Länder vorzubeugen. (vgl. Verfassungsgerichtshof des Landes Berlin, Beschluss vom 20. März 2019 – VerfGH 92/17, juris Rn. 21).

Die Antwort des Senats erfolgt insoweit als Verschlussache des Geheimhaltungsgrades „VS – Vertraulich“ nach § 5 Abs. 1 der Verschlussachenanweisung für die Behörden des Landes Berlin (VSA). Sie kann in der nächsten Sitzung des Ausschusses für Verfassungsschutz in entsprechend eingestufte Sitzung erteilt werden (§ 54 Abs. 1 und 2 der Geschäftsordnung des Abgeordnetenhauses iVm § 9 Abs. 1 der Geheimschutzordnung des Abgeordnetenhauses). Dem durch Art. 45 Abs. 1 Satz 1 der Verfassung von Berlin begründeten parlamentarischen Informationsrecht wird damit unter Berücksichtigung der berechtigten Geheimschutzinteressen des Senats Rechnung getragen.

7. Wie viele Datensätze von minderjährigen Personen aus Berlin befinden sich in den Datenbanksystemen des Verfassungsschutzes? Wie viele davon sind beim Stand der Anfrage noch unter 14 Jahre alt? Bitte vermerken Sie ebenfalls welche ermittlungsunterstützenden Hinweise (EHW) oder personengebundene Hinweise (PHW) jeweils vermerkt sind.

Zu 7.:

Zum Zeitpunkt des Eingangs der Anfrage sind Daten von 82 Personen gespeichert, die das 18. Lebensjahr nicht vollendet haben.

46 davon sind im Rahmen des gesetzlichen Beobachtungsauftrages des Berliner Verfassungsschutzes gespeichert. Es wurden 14 personengebundene Hinweise vergeben. Weitergehende Angaben können aus Rechtsgründen nicht im Rahmen einer Schriftlichen Anfrage erfolgen. Eine detaillierte Darlegung, welche personenbezogenen Hinweise durch den Berliner Verfassungsschutz sowie den Verfassungsschutzverbund zu den betroffenen minderjährigen Personen erfasst sind, würde angesichts der geringen Zahl der betroffenen Personen unmittelbare Rückschlüsse auf die Arbeitsweise und den Erkenntnisstand des Berliner Verfassungsschutzes sowie des Verfassungsschutzverbundes insgesamt zu einem bestimmten Personenkreis zulassen. Der Anspruch auf Beantwortung der Schriftlichen Anfrage wird insoweit durch die Belange des Staatswohls begrenzt, um Gefahren für die Sicherheit des Landes Berlin sowie des Bundes und der übrigen Länder vorzubeugen. (vgl. Verfassungsgerichtshof des Landes Berlin, Beschluss vom 20. März 2019 – VerfGH 92/17, juris Rn. 21). Auch die Persönlichkeitsrechte der betroffenen Minderjährigen sind in die Abwägung einzubeziehen. Die Antwort des Senats erfolgt insoweit als Verschlussache des Geheimhaltungsgrades „VS – Vertraulich“ nach § 5 Abs. 1 der Verschlussachenanweisung für die Behörden des Landes Berlin (VSA). Sie kann in der nächsten Sitzung des Ausschusses für Verfassungsschutz in entsprechend eingestufte Sitzung erteilt werden (§ 54 Abs. 1 und 2 der Geschäftsordnung des Abgeordnetenhauses iVm § 9 Abs. 1 der Geheimschutzordnung des Abgeordnetenhauses). Dem durch Art. 45 Abs. 1 Satz 1 der Verfassung von Berlin begründeten parlamentarischen Informationsrecht wird damit unter Berücksichtigung der berechtigten Geheimschutzinteressen des Senats Rechnung getragen.

Im Rahmen des gesetzlichen Beobachtungsauftrages sind gemäß § 12 des Gesetzes über den Verfassungsschutz in Berlin keine personenbezogenen Daten Minderjähriger gespeichert, die das 14. Lebensjahr nicht vollendet haben.

36 Personen, die das 18. Lebensjahr nicht vollendet haben, sind im Zusammenhang mit gesetzlichen Nachberichtspflichten in Mitwirkungsangelegenheiten bei gesetzlich vorgeschriebenen Überprüfungen anderer Stellen gespeichert (z.B. Zuverlässigkeitsüberprüfungen nach dem Luftsicherheits- oder Waffengesetz). Zwei davon haben das 14. Lebensjahr noch nicht vollendet.

8. Inwiefern werden bestehende Eintragungen in Hinblick auf möglicherweise diskriminierende Elemente kontrolliert und diese korrigiert? Wenn ja, durch wen geschieht dies und inwiefern werden die Beamt*innen, die diese Eintragungen vorgenommen hatten, über diese kritischen Inhalte aufgeklärt?

9. Was geschieht mit Daten nach Ablauf der Aufbewahrungsfristen? Inwiefern findet eine Löschung der Daten automatisch statt oder muss aktiv durch Mitarbeiter*innen durchgeführt werden? Wenn ja, durch wen erfolgt dies und inwiefern wird dies kontrolliert?

Zu 8. und 9.:

Es erfolgen nur Eintragungen, die für die gesetzliche Aufgabenerfüllung des Berliner Verfassungsschutzes erforderlich sind. Nach Ablauf der Speicherfrist werden die Daten gelöscht. Eine rechtzeitige Vorlage der Datensätze zur Erfüllung der gesetzlichen Prüf- und Löschpflichten wird grundsätzlich systemseitig sichergestellt. Darüber hinaus unterliegen die Datensätze der Qualitätskontrolle einer eigenen Arbeitseinheit, die als Daueraufgabe mit der Kontrolle der Speicher- bzw. Löschungsvoraussetzungen der Daten betraut ist.

10. In wie vielen Fällen wurden durch Bedienstete des Landesamts für Verfassungsschutz unbefugt, ohne dienstlichen Anlass, personenbezogene Daten aus den zugänglichen Datenbanksystemen des Amtes abgerufen? (Bitte für Fälle seit 2018, inklusive folgender Angaben, vermerken: Welche (personenbezogenen) Daten wurden unbefugt abgerufen? Wozu wurden diese Daten verwendet/abgerufen? Wie wurde mit den jeweiligen Fällen umgegangen? (Bitte Stand der (Strafrechtlichen-) Ermittlungen anführen bzw. angeben, welche (disziplinarrechtlichen) Sanktionen verhängt wurden)

Zu 10.:

Es ist ein Fall bekannt, in dem eine Dienstkraft unbefugt personenbezogene Daten abgefragt hat. Ihr wurde unverzüglich die Ermächtigung zum Umgang mit Verschlussachen entzogen und sie wurde nicht mehr im Berliner Verfassungsschutz eingesetzt. Weitergehende Angaben können zu einer Personaleinzelangelegenheit aus Rechtsgründen nicht erfolgen.

11. Inwiefern gab es Fälle, in denen durch Bedienstete des Landesamts für Verfassungsschutz personenbezogene Daten, die dienstlich erlangt wurden, im Nachgang für private Zweck missbraucht wurden? (Falls ja, bitte für Fälle seit 2018, inklusive folgender Angaben, vermerken: Welche (personenbezogenen) Daten wurden missbraucht? Wozu wurden diese Daten missbraucht? Wie wurde mit den jeweiligen Fällen umgegangen? (Bitte Stand der (Strafrechtlichen-) Ermittlungen anführen bzw. angeben, welche (disziplinarrechtlichen) Sanktionen verhängt wurden)

12. Wie hat sich die Gesamtanzahl dieser in Frage 10 und 11 behandelten Missbräuchen von (personenbezogenen) Daten in den letzten Jahren entwickelt? (Bitte jährliches Fallaufkommen seit 2011 auflisten.) Wie bewertet der Senat diese Entwicklungen?

13. Inwiefern hält der Senat die Maßnahmen im Umgang mit Beamt*innen, die sich unrechtmäßig Zugang zu (personenbezogenen) Daten verschafft haben, für ausreichend? Inwiefern sind hier Verschärfungen geplant?

14. Inwiefern haben einzelne Beamt*innen des Landesamts für Verfassungsschutz, mehrmalig unbefugt personenbezogene Daten abgerufen oder verwendet? Wenn ja bitte anfügen, wie viele Fälle den jeweiligen Bediensteten zuzuordnen sind und darstellen, wie mit diesen mehrmaligen Verstößen umgegangen wurde/wird.

15. Inwiefern wird ein Nachbesserungsbedarf bezüglich der Einhaltung des Datenschutzes und anderer Vorschriften im Umgang mit den Datensystemen gesehen, sowohl in technischer Hinsicht als auch in Hinblick auf die Unterweisung der Zugangsberechtigten und die Ausgestaltung und Kontrolle der Einhaltung der Weisungen?

Zu 11. bis 15.:

Daten im Sinne der Anfrage sind im automatisierten Verfahren nicht recherchierbar. Die bestehenden Maßnahmen gegen unbefugten Zugriff werden als ausreichend erachtet.

16. Inwiefern werden Bedienstete des Landesamts für Verfassungsschutz über datenschutzrechtliche Vorschriften informiert, belehrt und weitergebildet? Bitte untergliedern nach etwaigen Maßnahmen für Arbeitsplätze und mobile Endgeräte.

Zu 16.

Die Information, Belehrung und Weiterbildung über datenschutzrechtliche Vorschriften ist Bestandteil der vor Zugriffserteilung obligatorischen Schulungen der Dienstkräfte. Durch Fortbildungen werden diese bedarfsweise zu spezifischen Themenfeldern vertieft. Darüber hinaus können sich die Dienstkräfte jederzeit an den behördlichen Datenschutzbeauftragten wenden. Dieser informiert die Dienstkräfte erforderlichenfalls auch eigeninitiativ über wesentliche datenschutzrechtliche Änderungen.

Berlin, den 9. Februar 2024

In Vertretung

Christian Hochgrebe
Senatsverwaltung für Inneres und Sport