Abgeordnetenhaus BERLIN

Drucksache 18 / 25 141
Schriftliche Anfrage

18. Wahlperiode

Schriftliche Anfrage

der Abgeordneten Niklas Schrader und Anne Helm (LINKE)

vom 01. Oktober 2020 (Eingang beim Abgeordnetenhaus am 02. Oktober 2020)

zum Thema:

Personenabfragen in Polizeidatenbanken – Protokollierung und Schutz vor unbefugten Zugriffen

und **Antwort** vom 21. Oktober 2020 (Eingang beim Abgeordnetenhaus am 22. Okt. 2020)

Die Drucksachen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin, Telefon: 6 61 84 84; Telefax: 6 61 78 28.

Senatsverwaltung für Inneres und Sport

Herrn Abgeordneten Niklas Schrader (LINKE) und
Frau Abgeordnete Anne Helm (LINKE)
über
den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 18/25141
vom 1. Oktober 2020
über Personenabfragen in Polizeidatenbanken – Protokollierung und Schutz vor unbefugten Zugriffen

---

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

1. Wie oft und auf welche Weise genau müssen Polizeidienstkräfte bei Personenabfragen in den folgenden zugänglichen Datenbanken unter welchen Voraussetzungen den Anlass bzw. Grund ihrer Abfrage angeben?

a. das Polizeiliche Landessystem zur Information, Kommunikation und Sachbearbeitung (POLIKS)
b. das nationale Polizeisystem Inpol,
c. die Datenbanken des internationalen Verbunds Interpol,
d. das Schengener Informationssystem (SIS),
e. das Ausländerzentralregister (AZR) oder
f. das Visa-Informationssystem (VIS)
g. die europäische Fingerabdruckdatei Eurodac,
h. das Europol-Informationssystem,
i. die Sexualstraftäterdatei,
j. die „zentrale Haftbefehlssammlung und Indexdatei“,
k. die Fahrradhalter-Datenbank,
l. das Verzeichnis zu Wirtschaftskriminalität und
m. die Auswertedatenbank polizeilicher Staatsschutz

Zu 1. a. bis m.:
Personenabfragen in das
a. Polizeiliche Landessystem zur Information, Kommunikation und Sachbearbeitung (POLIKS),
b. Informationssystem der Polizei (INPOL),
d. Schengener Informationssystem (SIS),
e. Ausländerzentralregister (AZR) und
f. VISA-Informationssystem

erfolgen direkt aus POLIKS heraus. Hierbei ist für jede einzelne Abfrage ein katalogbasierter Abfragegrund auszuwählen, der durch einen Freitext ergänzt werden muss.

c. Bei jeder Personenabfrage im Verbund Interpol ist neben den bekannten Suchparametern – Vorname, Name, Geburtsdatum – auch die abfragende Dienststelle sowie

die der Abfrage zu Grunde liegende Vorgangs- oder Geschäftsnummer anzugeben. Über einen Zugriff verfügen nur Mitarbeitende, die auf Antrag vom Bundeskriminalamt (BKA) eine persönliche Zugangsberechtigung erhalten haben.

g. Als Grund einer Anfrage im System EURODAC wird die Rechtsgrundlage der im Kontext stehenden erkennungsdienstlichen Behandlung angegeben.

h. Abfragen im Europol-Informationssystem (EIS) erfolgen ausschließlich durch extra geschulte Polizeidienstkräfte über persönliche Zugangsberechtigungen. Es ist keine gesonderte Angabe des Abfrageanlasses oder -grundes für die Durchführung einer EIS-Abfrage erforderlich.

i. Bei der „Sexualstraftäterdatei“ handelt es sich um eine angemeldete Arbeitsdatei, die von einer Fachdienststelle mit wenigen Dienstkräften geführt wird. Nur die Mitarbeitenden dieser Dienststelle sind abfrageberechtigt. Bei einer Abfrage in dieser Datei wird kein Abfragegrund abverlangt.

j. Die Eingabe eines Abfrageanlasses beziehungsweise -grundes ist bei der Arbeit mit der „Haftbefehlssammlung“ systembedingt nicht erforderlich.

k. Für die Fahrradhalter-Datenbank ist keine Angabe eines Abfragegrundes nötig. Die Anfrage ist nur einem begrenzten Kreis von Berechtigten möglich. Die Fahrradhaltenden geben über eine Einwilligungserklärung ihre Zustimmung.

l. Sämtliche Daten, welche das Themenfeld der Wirtschaftskriminalität tangieren, werden in POLIKS eingepflegt – eine entsprechende Abfrage hieraus erfolgt unter den gleichen Voraussetzungen wie bei den übrigen POLIKS-Datenbeständen. Ein eigenständiges Verzeichnis im Sinne der Fragstellung gibt es nicht.

m. Die Nutzung der Datei „Auswertedatenbank polizeilicher Staatsschutz“ wurde im Jahr 2009 eingestellt. Seit diesem Zeitpunkt sind weder die Erfassung personenbezogener Daten noch deren Abfragen in dieser Datei möglich.

2. Welche Maßnahmen in Bezug auf Personenabfragen in den oben genannten polizeilichen Datenbanken plant die Polizei derzeit, damit diese sich im Rahmen einer etwaigen nachträglichen Revision oder datenschutzrechtlichen Überprüfung einwand- und zweifelsfrei dienstlich begründen lassen?

Zu 2.:
Die für die Zugriffskontrolle implementierten technischen und organisatorischen Maßnahmen wurden und werden gemäß § 32 Abs. 1 Nr. 5, § 50 Abs. 3 Satz 1 des Berliner Datenschutzgesetzes (BlnDSG) als ausreichend und angemessen erachtet.

Das derzeitige Verfahren sichert den Zugang zur Datenbank technisch ab, hinzu kommt ein auf das Aufgabengebiet der Nutzenden individuell angepasstes Rollen- und Rechtekonzept, welches nur den Zugriff auf die zur Aufgabenerfüllung notwendigen Daten zulässt. Für die Rechtmäßigkeit der jeweiligen Abfrage ist die Dienstkraft selbst verantwortlich. Jede Abfrage im POLIKS (siehe auch Antworten zu 1. a), b), d), e), f) sowie in der „Sexualstraftäterdatei“ (1. i)) wird in einem Datenschutzprotokoll aufgezeichnet, so dass eine Überprüfung jederzeit möglich ist.

Für die Protokollierung von Abfragen über Online-/ Web-Portale oder Ähnliches (Datenbanken zu 1. c), g), h) ist die jeweilige betreibende Stelle verantwortlich. Dies obliegt nicht der Polizei Berlin.

In fachbezogenen Arbeitsdateien wie den unter 1. j) und k) genannten, findet keine Zugriffsprotokollierung statt. In der Fahrradhalterdatenbank (1. k) wird das Erfassen und Bearbeiten von personenbezogenen Daten protokolliert.
Darüber hinaus besteht die Möglichkeit, Vorgänge durch die Vorgangsverantwortlichen in die Vorgangsüberwachung zu stellen und somit zu erkennen, wer ggf. unberechtigt auf diesen Vorgang zugegriffen hat.

Die Polizei Berlin hat einen Verbesserungsvorschlag der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) aufgenommen und wird das bereits existierende Zusatzfeld, in welchem der Abfragegrund bei polizeilichen Abfragen im POLIKS ergänzt wird, dahingehend weiter ausgestalten, dass grundsätzlich eine Vorgangsnummer einzutragen ist und, wenn dies nicht möglich ist, zumindest eine Plausibilitätsprüfung der Ziffern- bzw. Buchstabenfolge des eingegebenen Freitextes erfolgt. Somit wird die abfragende Dienstkraft angehalten, den bereits ausgewählten Abfragegrund plausibel zu ergänzen. Aufgrund notwendiger Programmierarbeiten durch eine beauftragte Firma kann die Umsetzung bis zum Frühjahr 2021 dauern.

3. Mit welchen Maßnahmen (TAN-Verfahren, Zwei-Faktor-Authentifizierung etc.) wird derzeit sichergestellt, dass unbefugte Dienstkräfte über den Multifunktionalen Arbeitsplatz (MAP) keinen Zugriff auf Nutzer*innenkonten und damit möglicherweise polizeiliche Datenbanken haben, für die sie nicht die erforderlichen Berechtigungen besitzen?

Zu 3.:
MAP-Nutzende verfügen über eine individuelle Nutzerkennung sowie ein von ihnen vergebenes Passwort. Sie sind verpflichtet, diese Daten unter Verschluss zu halten und dürfen sie niemandem zur Verfügung stellen. Zusätzlich ist für jede Datenbank ein Rollen- und Rechtekonzept hinterlegt, welches individuell den Zugriff regelt.

3.a. Nach welcher Inaktivitätszeit am MAP erfolgt gegebenenfalls eine automatische Abmeldung vom Nutzer*innenkonto?

Zu 3.a.:
Als Voreinstellung schaltet sich nach 15 Minuten Inaktivität der Bildschirmschoner ein, der nur nach Eingabe des Passwortes entsperrt werden kann. Diese Zeit kann durch die Nutzenden individuell verkürzt werden. Darüber hinaus ist jede Dienstkraft verpflichtet, beim Verlassen ihres Arbeitsplatzes den Rechner gegen unbefugten Zugriff zu sperren.

3.b. Welche Komplexitätsanforderungen gelten für Passwörter, die von Polizeidienstkräften für den Zugang zum MAP frei gewählt werden?

Zu 3.b.:
Laut der geltenden Passwortrichtlinie muss ein Passwort eine Mindestlänge von 10 Zeichen sowie je einen Groß-, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten.

3.c. In welchen zeitlichen Abständen müssen Passwörter gegebenenfalls regelmäßig geändert werden?

Zu 3.c.:
Im Wege der Usability und Gebrauchstauglichkeit wird den Dienstkräften die Häufigkeit der Änderung des Zugangskennwortes in eigener Verantwortung übertragen, allerdings hinsichtlich der Komplexitätsanforderungen ein sicherer Standard erzwungen (s. Antwort zu Frage 3b). Ein häufiges Erzwingen des Kennwortwechsels inklusive der festgelegten Passworthistorie (Wiederholungsverbotsregel) führt dazu, dass die Kennwörter von den Mitarbeitenden unsicher aufgeschrieben oder anderweitig gespeichert werden. Es kann jedoch von den Nutzenden anlassbezogen jederzeit geändert werden.

4. Welche verschiedenen Maßnahmen zur Verbesserung der Sicherheit von IT-Systemen plant die Polizei derzeit im Einzelnen, damit rechtswidrige Zugriffe auf personenbezogene Daten in Polizeidatenbanken ausgeschlossen werden? (Bitte ausführen.)

Zu 4.:
Eine technische Überprüfung der Rechtmäßigkeit der einzelnen Abfrage ist, anders als der grundsätzliche Zugang zu den IT-Systemen, nicht möglich und unterliegt stattdessen der Verantwortung der Abfragenden.

5. Gegen wie viele Polizeidienstkräfte wird derzeit wegen Verstoßes gegen das Landesdatenschutzgesetz ermittelt?

Zu 5.:
Die folgenden Fallzahlen beruhen auf verlaufsstatistischen Daten des Systems Data Warehouse Führungsinformation (DWH FI). Es handelt sich um Daten, die den tagesaktuellen Stand der im POLIKS erfassten Vorgänge abbilden. Da es sich um eine Eingangsstatistik handelt, können sich aufgrund möglicher Änderungen der Erfassungsgründe im Ermittlungsverlauf geringfügige Abweichungen ergeben.
Im LKA 34 wird momentan in vier Ermittlungsverfahren gegen Polizeimitarbeitende wegen des Verdachts des Verstoßes gegen das Landesdatenschutzgesetz ermittelt. In zwei Vorgängen ist je eine Polizeidienstkraft namentlich bekannt. In den anderen beiden Verfahren werden die Ermittlungen zu jeweils einer noch unbekannten Person geführt (Quelle: DWH FI, Stand: 15. Oktober 2020, 09:50 Uhr).
Im Übrigen wird auf die Ausführungen zu Frage 6 verwiesen.

6. Wie viele Disziplinarverfahren und Strafermittlungsverfahren gegen Polizeidienstkräfte wegen des Verdachts auf Verstoß gegen das Landesdatenschutzgesetz sind jeweils in den Jahren seit 2015 mit welchen jeweiligen Ergebnissen abgeschlossen worden?

Zu 6.:
Die erfragten Abschlüsse von Disziplinarverfahren wegen Verstoßes gegen das Landesdatenschutzgesetz werden weder zahlenmäßig noch nach ihrem jeweiligen Ergebnis statistisch gesondert ausgewiesen.
Grundsätzlich lassen sich Strafermittlungsverfahren wegen Verstoßes gegen das Berliner Datenschutzgesetz im staatsanwaltschaftlichen Registratursystem MESTA zwar über das Delikt ermitteln. Der Beruf der Beschuldigten wird im MESTA jedoch nicht gespeichert, sodass sich eine Begrenzung auf Polizeidienstkräfte als Beschuldigte nicht erreichen lässt und eine genaue Auskunft aus MESTA daher nicht möglich ist.
Wertet man das System auf Verfahren wegen Verstoßes gegen das Berliner Datenschutzgesetz und mit dem Sachgebietsschlüssel „Zwang und Missbrauch des Amtes

durch Polizeibedienstete“ aus, kommt man zu folgenden, ggfs. nicht ganz vollständigen Ergebnissen:
2015: insgesamt zwei Verfahren, die gemäß § 170 II StPO eingestellt wurden.
2016: insgesamt ein Verfahren, das gemäß § 170 II StPO eingestellt wurde.
2017: kein Verfahren.
2018: insgesamt zwei Verfahren, von denen je eins gemäß § 170 II StPO bzw. § 153 Abs. 1 Satz 2 Nr. 2 StPO eingestellt wurde.
2019: insgesamt zwei Verfahren, die jeweils als Ordnungswidrigkeitenverfahren an die zuständigen Behörden abgegeben wurden.
2020: insgesamt drei Verfahren, von denen zwei noch offen sind und das dritte zur Ahndung als Ordnungswidrigkeit an die Berliner Beauftragte für Datenschutz und Informationsfreiheit abgegeben wurde.

7. Bei wie vielen Betroffenen der rechten Neuköllner Anschlagsserie wurde bisher wann und mit welchen jeweiligen Ergebnissen geprüft, ob im zeitlichen Umfeld der gegen sie als Geschädigte gerichteten Straftaten unbegründete Abfragen ihrer personenbezogenen Daten in Polizeidatenbanken vorgenommen wurden?
a. Wie viele unbegründete Abfragen ihrer personenbezogenen Daten in Polizeidatenbanken gab es bei wie vielen Betroffenen der rechten Neuköllner Anschlagsserie?
b. Welche und wie viele der Anfragen wurden vor und welche nach den gegen sie gerichteten Straftaten festgestellt?

Zu 7 a bis b.:
Die Ermittlungen der Generalstaatsanwaltschaft Berlin in den von der Staatsanwaltschaft Berlin übernommenen Verfahren zum Komplex „Neuköllner Anschlagsserie“ dauern nach deren Wiederaufnahme an.
Daher kommen diesbezügliche Auskünfte derzeit zum Schutze des Untersuchungszwecks nicht in Betracht.

8. Welche Maßnahmen bezüglich der Zugriffsprotokollierung hat die Polizei seit dem Erscheinen des Berichts der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BlnBDI) 2019, demzufolge das polizeiliche System zur Personensuche rechtswidrig ist, im Einzelnen umgesetzt? (Bitte jeweils einzeln auflisten und erläutern.)

Zu 8.:
Auf die Beantwortung zu Frage 2 wird verwiesen.

9. Hat die Polizei die seit Juni 2013 suspendierte automatisierte Löschung personenbezogener Daten in POLIKS wieder aufgenommen? Wenn ja, wann? Wenn nein, aus welchen Gründen nicht?

Zu 9.:
Da das Löschmoratorium nach wie vor in Kraft ist, werden keine Daten aus dem POLIKS automatisiert gelöscht.

10. Auf welche Weise wurden bisher wie viele löschreife, jedoch aufgrund der Löschmoratorien für die Untersuchungsausschüsse zum Breitscheidplatz-Attentat und zum NSU-Komplex fortdauernd gespeicherte Datensätze zumindest zugriffsbeschränkt?

Zu 10.:
Durch einen automatisierten Prozess, bei dem jeder einzelne zur Löschung anstehende Vorgang maschinell geprüft wird, werden die Vorgänge vom Informationssystem abgekoppelt, d. h. die Referenz zwischen genau diesem Vorgang und den sonstigen Informationen zu dieser Person wird gelöscht. Danach werden die Vorgänge in

einen Schutzbereich „Datensperrung“ verschoben. Nur eine geringe Anzahl Mitarbeitender hat Zugriff zu diesem Bereich und auf diese Vorgänge. Für alle anderen Anfragenden sind diese Vorgänge vollständig unsichtbar und nicht mehr über eine Personen- oder Vorgangsabfrage zu ermitteln.

Bisher wurden rund 4,8 Millionen Vorgänge in den Schutzbereich verschoben, ca. 700.000 stehen noch aus.

11. Auf welche genaue Weise wurde seit dem BlnBDI-Bericht aus dem Jahr 2019 bei der Zugriffskontrolle gegebenenfalls ein Stichprobenverfahren eingeführt, das inhaltlich von einer organisatorisch sowie thematisch getrennten und somit unabhängigen Stelle durchgeführt wird?

Zu 11.:
Eine regelmäßige Zugriffskontrolle erfolgt im Rahmen von stichprobenartigen verdachtsunabhängigen Datenschutzkontrollen bereits seit 2004 durch den behördlichen Datenschutzbereich im Justiziariat des Polizeipräsidiums. Das diesbezügliche in einer Dienstvereinbarung mit dem Gesamtpersonalrat geregelte Verfahren befindet sich gerade in der Prüfung und Überarbeitung.

12. In welchem Umfang umfassen die aufgrund der NSU-Untersuchungsausschüsse und des Untersuchungsausschusses zum Breitscheidplatz-Attentat eingerichteten Löschmoratorien auch die protokollierten Zugriffe auf die vorgehaltenen personenbezogenen Daten durch Polizeidienstkräfte?

Zu 12.:
Die Aufbewahrungsfrist für die Protokolldaten beträgt im Normalfall zwei Jahre, dann werden sie gelöscht.
Um den Auskunftsbedürfnissen der Untersuchungsausschüsse nachzukommen, werden die älteren Protokolldaten exklusiv für diesen Zweck bis zur Aufhebung des Löschmoratoriums gespeichert.

13. Ist das Disziplinarverfahren gegen den Polizeibeamten Sebastian K., der am 21. Dezember 2017 Drohbriefe unter anderem gegen vermeintliche Angehörige der linken Szene versandt hat, bereits abgeschlossen und wenn ja, mit welchem Ergebnis, und welche dienstrechtlichen Schritte sind ggf. eingeleitet worden?

14. In welcher polizeilichen Dienststelle wird der Polizeibeamte Sebastian K. gegenwärtig verwendet?

Zu 13. und 14.:
Das Disziplinarverfahren ist abgeschlossen. Im Übrigen wird aus fürsorge- und datenschutzrechtlichen Gründen zu Personaleinzelangelegenheiten keine Stellung genommen.

15. Konnte die polizeiliche Abfrage der personenbezogenen Daten der Künstlerin B. am 5. März 2019, die wenige Tage später ein Drohschreiben mit Bezugnahme auf einen „NSU 2.0“ erhielt, einer bestimmten Polizeidienstkraft zugeordnet werden?
a. Wenn nein, aus welchen genauen Gründen nicht?
b. Wegen welcher Tatbestände wurde anlässlich der Abfrage gegebenenfalls ein Disziplinarverfahren oder Strafermittlungsverfahren eingeleitet?
c. Von welcher polizeilichen Dienststelle wurde die Abfrage gegebenenfalls vorgenommen?
d. Welche polizeilichen Maßnahmen (Hausdurchsuchungen, Sicherstellung von Datenträgern etc.) wurden gegebenenfalls bereits gegen den bzw. die Tatverdächtigen mit welchen jeweiligen Ergebnissen vorgenommen?

16. Welche Anhaltspunkte für eine Vernetzung in welche Polizei- oder Sicherheitsbehörden anderer Bundesländer oder des Bundes sieht der Senat bei den Tatverdächtigen der unbefugten polizeilichen Personensuchen in Datenbanken, in deren Folge „NSU 2.0“-Drohschreiben mit den entsprechenden Personendaten auftauchten?

17. Wie viele Dienstkräfte welcher Dienststellen bzw. polizeilichen Untergliederungseinheiten ermitteln derzeit zu den unter Frage 15 und 16 genannten Sachverhalten?

Zu 15. a. bis d., 16. und 17.:
Die Fragen beziehen sich auf ein laufendes Ermittlungsverfahren der Staatsanwaltschaft Frankfurt am Main, sodass Auskünfte ausschließlich von dort aus erteilt werden können. Das LKA Berlin war in Amtshilfe tätig.
Es wurde kein Disziplinarverfahren auf Grund einer Abfrage der Künstlerin B. eingeleitet.

Berlin, den 21. Oktober 2020

In Vertretung

Torsten Akmann
Senatsverwaltung für Inneres und Sport