Abgeordnetenhaus BERLIN

Drucksache 19 / 18 091
Schriftliche Anfrage

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:

POLIKS II: Verstöße gegen Datenschutzregeln und andere Vorschriften

und **Antwort** vom 18. Februar 2024 (Eingang beim Abgeordnetenhaus am 20. Februar 2024)

Senatsverwaltung für Inneres und Sport

Frau Abgeordnete Gollaleh Ahmadi (GRÜNE) und
Frau Abgeordnete June Tomiak (GRÜNE)

über
die Präsidentin des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/18 091
vom 30. Januar 2024
über POLIKS II: Verstöße gegen Datenschutzregeln und andere Vorschriften
---

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

1. Wie schätzt der Senat die Einhaltung des Datenschutzes beim Umgang mit POLIKS und anderen Datensystemen, auf die die Berliner Polizei Zugriff hat (z. B. aus anderen Bundesländern), ein?

Zu 1.:
Die Einhaltung des Datenschutzes im Umgang mit dem polizeilichen Landessystem zur Information, Kommunikation und Sachbearbeitung (POLIKS) wird als hoch eingeschätzt. Insbesondere wurde die Sicherheit bei POLIKS durch weitere technisch-organisatorische Maßnahmen erhöht. In der Regel erfolgt der Zugriff auf Fremdsysteme über das Auskunftssystem in POLIKS. Der Zugriff auf POLIKS und andere Datensysteme ist gesetzlich geregelt und wird protokolliert.

2. Inwiefern werden Polizeikräfte in Hinblick auf datenschutzrechtliche und andere Vorschriften und Weisungen im Umgang mit POLIKS und anderen Datensystemen geschult und weitergebildet?

Zu 2.:
Anwärterinnen und Anwärtern des mittleren Polizeivollzugsdienstes werden die einschlägigen Vorschriften für Datenabgleiche in POLIKS, § 28 des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG Bln) und § 98c der Strafprozessordnung (StPO)

auch in Verbindung mit § 46 Absatz1 des Gesetzes über Ordnungswidrigkeiten (OWiG) im Rahmen des Eingriffsrechts-Unterrichtes vermittelt. Darüber hinaus werden die Auszubildenden auf weitere, spezielle Datenabfragesysteme hingewiesen, auf die die Polizei Berlin über entsprechende Schnittstellen Zugriff hat (z. B. Schengener Informationssystem, Einwohnerwesen). Insbesondere werden die Grundsätze „nur zu dienstlichen Zwecken“ und „es muss immer ein konkreter Abfragegrund vorliegen“ betont.

Im Rahmen der kriminalistischen Ausbildung („Informationssysteme und Auskunftsdienste“) befassen sich die Nachwuchskräfte mit den hier in Rede stehenden Auskunftssystemen, die ihnen dienstlich relevante Informationen zur Verfügung stellen. Hierbei werden die Nachwuchskräfte auch insbesondere bezüglich nachfolgend aufgeführter Punkte des Datenschutzes sensibilisiert:

- jeder Zugriff auf Daten muss auf einer Rechtsgrundlage basieren und darf nur aus dienstlichem Grund erfolgen,
- jeder Zugriff wird protokolliert,
- Verstöße dagegen können Dienstvergehen darstellen und disziplinarisch geahndet werden bzw. unter Umständen auch Straftatbestände verwirklichen.

Anwärterinnen und Anwärter des gehobenen Polizeivollzugsdienstes werden im Rahmen ihres Bachelorstudienganges an der Hochschule für Wirtschaft und Recht Berlin sowohl im fachtheoretischen als auch im fachpraktischen Bereich im Hinblick auf datenschutzrechtliche und andere Vorschriften und Weisungen im Umgang mit POLIKS und anderen Datensystemen ausgebildet. Insbesondere im Unterrichtsmodul 10 „Polizei- und Ordnungsrecht II“ werden den Studierenden die grundlegenden Prinzipien des nationalen und europäischen Datenschutzrechtes und Kenntnisse der übrigen gesetzlichen Regelungen über die Eingriffsmaßnahmen der polizeilichen Datenverarbeitung anwendungssicher vermittelt. Darüber hinaus wird die Thematik auch unter dem Aspekt der Grund- und Menschenrechte (Modul 7) im Rahmen des allgemeinen Persönlichkeitsrechts, des Rechts auf informationelle Selbstbestimmung sowie der Vertraulichkeit und Integrität informationeller Systeme, des Schutzes personenbezogener Daten sowie des Privatlebens eingehend behandelt.

Ein Schwerpunkt der fachpraktischen Ausbildung aller Nachwuchskräfte, aber auch der Fortbildung bezüglich POLIKS und der damit verknüpften Auskunftssysteme liegt in der Vermittlung der datenschutzrechtlichen Vorschriften und Weisungen wie beispielsweise der Vermittlung der dezidierten Ergänzung des Abfragegrundes im Rahmen der Erlangung von Auskünften. Darüber hinaus erfolgt eine jährliche Bekanntgabe der entsprechenden Vorschriften gegen Unterschrift.

3. Inwiefern sind auch Personen jenseits der Dienstkräfte der Berliner Polizei befugt, Daten über POLIKS oder andere Datensysteme abzufragen und wenn ja, wie erfolgt hier die Unterweisung und Weiterbildung zu daten-schutzrechtlichen oder anderen Vorschriften?

Zu 3.:
Polizeidienstkräfte eines anderen Landes, des Bundes sowie Zollbedienstete haben unter den Voraussetzungen des § 8 ASOG Bln die gleichen Befugnisse wie Polizeidienstkräfte des Landes Berlin. Ferner haben bestimmte Polizeidienstkräfte des Landes Brandenburg und der Bundespolizei, die jeweils in einer gemeinsamen Ermittlungsgruppe mit der Berliner Polizei zusammenarbeiten, Zugriff auf POLIKS auf der Grundlage einer Rechtsverordnung nach § 46 Absatz 4 ASOG.

Eine Berechtigung zum Zugriff auf POLIKS erfolgt grundsätzlich erst nach erfolgreicher Teilnahme an einer entsprechenden Schulung. Allen zuvor genannten Dienstkräften wurden ebenfalls die datenschutzrechtlichen Vorschriften und Weisungen vermittelt.

4. Inwiefern wird ein Nachbesserungsbedarf bezüglich der Einhaltung des Datenschutzes und anderer Vorschriften im Umgang mit POLIKS und anderen 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 4.:
In den vergangenen Jahren erfolgte die weitere Implementierung technisch-organisatorischer Maßnahmen – insbesondere die Anpassung der Weisungslage. Darüber hinaus erfolgte eine weitere Ausgestaltung der anlassunabhängigen Kontrollen. Diese technisch-organisatorischen Maßnahmen werden stetig evaluiert und ggf. angepasst.

5. Wie wird sichergestellt, dass es weder bei festen Arbeitsplätzen, noch mobilen Anwendungen Zugriff auf Daten von POLIKS oder vergleichbaren Datensystemen durch unbefugte Dritte kommen kann, z.B. über eine Zwei-Faktor-Authentifizierung oder andere Arten von Zugangskontrollen? Inwiefern gibt es hierbei Unterschiede zu anderen Datensystemen?

Zu 5.:
Der Zugang zu einem festen Arbeitsplatz innerhalb von polizeilichen Liegenschaften wird über Benutzerkennung und Passwort sichergestellt. Im Falle mobiler Nutzung von dienstlichen Notebooks erfolgt der Zugang mittels Zwei-Faktor-Authentifizierung. Dienstliche Smartphones und Tablets sind durch eine PIN und ein weiteres Passwort gesichert. Der Zugang zu Fremdsystemen erfolgt in der Regel über eine der drei vorgenannten Möglichkeiten. Insofern bestehen keine Unterschiede.

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

Zu 6.:
Seit Januar 2018 wurde der Verlust von 41 mobilen Geräten gemeldet. Der Schutz vor unbefugten Zugriffen erfolgt insbesondere durch die Zwei-Faktor-Authentifizierung, wie bereits in der Beantwortung zu Frage 5 dargestellt. Im Verlustfall können Smartphones und Tablets geortet, gesperrt und in den Werkszustand zurückgesetzt werden. Notebooks verfügen zusätzlich über eine verschlüsselte Festplatte und können ebenfalls gesperrt werden.

7. Inwiefern werden Zugriffe auf POLIKS und andere Datenbanken über mobile Anwendungen und feste Arbeitsplätze erfasst bzw. kontrolliert und inwiefern und durch wen wird dies überwacht? Inwiefern lässt sich auf diesem Wege feststellen, ob unbefugte Dritte an Daten von POLIKS oder anderen Datenbanken gelangt sind? (Falls solche Daten vorliegen, bitte nach Jahren seit 2018, Art des Zugriffs (mobil oder fester Arbeitsplatz) und Gegenstand der Abfrage aufschlüsseln)

Zu 7.:
Sämtliche Datenzugriffe in POLIKS werden in einer Protokolldatenbank aufgezeichnet. Die Aufzeichnungen können anlassbezogen ausgewertet werden. Zusätzlich erfolgt eine dauerhafte und ständige stichprobenartige Auswertung durch innerbehördliche Kontrollmechanismen. Bislang wurden keine Fälle von Nutzungen des polizeilichen Datennetzes durch unbefugte Personen bekannt.

8. Inwiefern wurden unrechtmäßige Abfragen, Abfragen mit Verstößen gegen datenschutzrechtliche Bestimmungen oder andere interne Weisungsregelungen beim Zugriff auf POLIKS-und andere Datenbanken seit 2018 erfasst? (Bitte aufschlüsseln nach Schutz- und Kriminalpolizei, Jahren, Art des Verstoßes und betroffenen personenbezogenen Daten)

Zu 8.:
Statistische Zahlen zu Datenschutzverstößen liegen erst ab dem Jahr 2020 vor. Ein Filtern speziell nach dem Verfahren POLIKS ist nicht möglich. Seit dem 28. September 2023 werden neben strafrechtlich relevanten Sachverhalten auch Verfahren erfasst, die aufgrund eines möglichen ordnungswidrigen Fehlverhaltens an die Berliner Beauftragte für Datenschutz und Informationsfreiheit übersandt wurden. Die statistisch erfassten Datenschutzverstöße können der folgenden Tabelle entnommen werden:

Jahr	Datenschutzverstöße
2020	15 Strafverfahren, davon 1 x § 153 a StPO Geldauflage, 3 x § 152 II StPO Anklagebehörde Staatsanwaltschaft,

	11 x § 170 II StPO Einstellung des Verfahrens.
2021	15 Strafverfahren, davon 1 x § 153 StPO Absehen der Verfolgung bei Geringfügigkeit, 14 x § 170 II StPO Einstellung des Verfahrens.
2022	15 Strafverfahren, davon 3 x noch offen 1 x § 152 II StPO Anklagebehörde Staatsanwaltschaft, 1 x § 153a StPO Geldauflage, 10 x § 170 II StPO Einstellung des Verfahrens.
2023	20 Strafverfahren, davon 11 x noch offen, 9 x § 170 II StPO Einstellung des Verfahrens.
2024	0 Strafverfahren, 3 x Abgabe an die Berliner Beauftragte für Datenschutz und Informationsfreiheit zur Prüfung eines Ordnungswidrigkeitenverfahrens.

Quelle: Interne Datenerhebung Polizeipräsidium Interne Revision 2, Stand: 2. Februar 2024

9. Inwiefern bestehen nach Einschätzung des Senats strukturelle Mängel beim polizeilichen Datenschutz bzw. den Sicherheitsvorgaben?

Zu 9.:
Der polizeiliche Datenschutz weist keine strukturellen Mängel auf.

10. Inwiefern kam es seit 2018 zu Fällen, bei denen Polizeibeamt*innen Daten aus POLIKS oder andere Datenbanken für widerrechtliche oder kriminelle Zwecke benutzt haben, vgl. Bericht der Berliner Datenschutzbeauftragten 2021 sowie der Fall, bei dem Drohbriefe an Aktivist*innen der linken Szene verschickt wurden? Welche straf- oder disziplinarrechtlichen Maßnahmen wurden gegen Beamt*innen ergriffen, bei denen es zu solchen Vorfällen kam?[1] (Bitte aufschlüsseln nach Schutz- und Kriminalpolizei, Jahren, Verstoß bzw. Straftatbestand und etwaiger Sanktion)

Zu 10.:
Eine statistische Erhebung von Daten im Sinne der Fragestellung erfolgt bei der Polizei Berlin nicht.

11. Wie positioniert sich der Senat zu dem Vorwurf, dass es aufgrund von unzureichend durchgesetzten Datenschutzvorschriften zu Fällen kam, in denen Tatverdächtige bzw. Täter*innen Zugriff auf die Daten

[1] Vgl. auch Artikel Berliner Zeitung vom 23.06.2022: Andreas Kopietz, „Berliner Polizisten spähten Verwandte, Freunde und Ex-Partner aus“, https://www.berliner-zeitung.de/mensch-metropole/neugierige-berliner-polizisten-spaehten-verwandte-und-freunde-aus-li.239192 (Zugriff 19.01.2024)

der mutmaßlichen Opfer oder Zeug*innen bekommen haben? (Bitte aufschlüsseln nach Schutz- und Kriminalpolizei, Jahren und den jeweils ermittelten Delikten)

Zu 11.:
Siehe Beantwortung zu Frage 4. Eine statistische Erhebung von darüberhinausgehenden Daten im Sinne der Fragestellung erfolgt bei der Polizei Berlin nicht.

12. Inwiefern hält der Senat die Maßnahmen im Umgang mit Beamt*innen, die sich – insbesondere wiederholt - regelwidrig oder unrechtmäßig Zugang zu Daten über POLIKS oder andere Datenbankensystemen verschafft haben, für ausreichend? Inwiefern sind hier Verschärfungen geplant?

Zu 12.:
Das Disziplinargesetz (DiszG) enthält im § 5 folgende Disziplinarmaßnahmen: Verweis, Geldbuße, Kürzung der Dienstbezüge, Zurückstufung und Entfernung aus dem Beamtenverhältnis. Darüberhinausgehende Maßnahmen sind weder vorgesehen noch erforderlich, um auf das Verhalten von Beamtinnen und Beamten einzuwirken. Entscheidend sind stets die Schwere des Dienstvergehens und die besonderen Umstände des Einzelfalls.

13. Inwiefern treffen Berichte zu, dass Dienstkräften seit Juli 2023 bei wiederholten Verstößen gegen Vorschriften im Umgang mit POLIKS und anderen Datenbankensystemen deutlich stärkere Sanktionen drohen, welche sind das und inwiefern kam es bereits zu solchen Sanktionen? (Bitte aufschlüsseln nach Schutz- und Kriminalpolizei, Verstoß und Sanktion aufschlüsseln)

Zu 13.:
Dienstpflichtverletzungen im Zusammenhang mit POLIKS und anderen Datenbanksystemen werden konsequent verfolgt und streng geahndet. Eine behördeneinheitliche Vorgehensweise wird unter der immer erforderlichen Prüfung im Einzelfall angestrebt. Bei wiederholten Verstößen ist aus Gründen der Verhältnismäßigkeit eine stufenweise Steigerung der Disziplinarmaßnahmen stets zu beachten. Dieser Grundsatz kam bereits vor Juli 2023 zur Anwendung.

14. Welche Maßnahmen und Änderungen im Umgang mit POLIKS (z.B. Weisungen, Kontrollen) sowie bei der Gestaltung der Bedienplattform wurden seit den wiederholten Vorwürfen zu Datenschutzverletzungen und Verstößen gegen interne Weisungen unternommen, und wie schätzt der Senat deren Wirksamkeit ein? Inwiefern gilt dies auch für andere Datensysteme, auf die die Berliner Polizei Zugriff hat?
15. Inwiefern sieht der Senat weiteren Nachbesserungsbedarf hinsichtlich der Gewährleistung eines angemessenen Schutzniveaus bei der Verarbeitung personenbezogener Daten in polizeilichen Datensystemen, z.B. durch technische Sicherheitsvorgaben oder sonstige organisatorische Maßnahmen?

Zu 14. und 15.:

Siehe Antwort zur Frage 4.

16. Inwiefern trifft es zu, dass die EU-Kommission ein Vertragsverletzungsverfahren wegen unzureichendem Datenschutz bei der Strafverfolgung eingeleitet hat, wie positioniert sich der Senat hierzu und wie ist der aktuelle Stand des Verfahrens?[2]

Zu 16.:
Es ist zutreffend, dass die EU-Kommission wegen der Umsetzung der Richtlinie (EU) 2016/680 (sog. JI-Richtlinie) ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet hat. Von dem Vertragsverletzungsverfahren ist in Teilen unter anderem auch das Berliner Landesrecht in Gestalt der Regelung des § 13 Absatz 2 des Berliner Datenschutzgesetzes (BlnDSG), der wortgleich mit § 16 Absatz 2 Bundesdatenschutzgesetz (BDSG) ist, hinsichtlich der datenschutzrechtlichen Abhilfebefugnisse der Berliner Beauftragten für Datenschutz und Informationsfreiheit im Bereich Justiz und Inneres betroffen.

Die Bundesregierung hat gegenüber der EU-Kommission am 19. Juli 2022 eine Stellungnahme abgegeben, in der sie ausführlich darlegt, dass Deutschland nicht gegen seine Verpflichtungen nach Artikel 47 Absatz 2 der JI-Richtlinie verstoßen hat, da es die Datenschutzaufsichtsbehörden im Bund und in den Ländern unter Ausschöpfung des bei der Umsetzung der Richtlinie gegebenen Regelungsspielraumes und unter Berücksichtigung des sensiblen Bereichs der Verhütung und Verfolgung von Straftaten mit wirksamen Abhilfebefugnissen ausgestattet hat.

Eine Reaktion der EU-Kommission hierauf ist nach Kenntnis des Senats bisher nicht erfolgt.

Berlin, den 18. Februar 2024

In Vertretung

Christian Hochgrebe
Senatsverwaltung für Inneres und Sport

[2] Vgl. Heise: Stefan Krempl: „Datenschutz bei Polizei: Neues EU-Vertragsverletzungsverfahren gegen Deutschland“, https://www.heise.de/news/Datenschutz-bei-Polizei-Neues-EU-Vertragsverletzungsverfahren-gegen-Deutschland-6666483.html (Zugriff 25.01.2024)