Bayerisches Staatsministerium des
Innern, für Sport und Integration

Bayerisches Staatsministerium des Innern, für Sport und Integration
80524 München

Präsidentin
des Bayer. Landtags
Frau Ilse Aigner, MdL
Maximilianeum
81627 München

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen	München
PI/G-4255-3/1189 I 19.10.2020	C5-0016-1-1044	15.12.2020

Schriftliche Anfrage der Abgeordneten Katharina Schulze vom 15.10.2020 betreffend Kontrolle unrechtmäßiger Datenbankabfragen durch bayerische Sicherheitsbehörden

Sehr geehrte Frau Landtagspräsidentin,

die Schriftliche Anfrage beantworte ich wie folgt:

zu 1.1.

Welche Kontrollmechanismen existieren für die verschiedenen bayerischen Polizeibehörden zur Erfassung bzw. Verhinderung von unrechtmäßigen Datenabfragen aus den polizeilichen Verbund- und Zentraldateien?

zu 2.1.

Welche technischen Sicherungssysteme werden von den bayerischen Polizeibehörden zur Verhinderung missbräuchlicher Zugriffe genutzt?

zu 2.2.

Welche Regelungen existieren für die Zugriffsberechtigung im Hinblick auf personenbezogene Daten aus den polizeilichen Verbund- und Zentraldateien?

Telefon: 089 2192-01 E-Mail: poststelle@stmi.bayern.de Odeonsplatz 3 · 80539 München
Telefax: 089 2192-12225 Internet: www.innenministerium.bayern.de U3, U4, U5, U6, Bus 100 (Odeonspl.)

zu 2.3.
Existiert in den einzelnen Organisationseinheiten ein detailliertes Rechte- und Rollenkonzept für den Zugriff auf sensible Datei- und Informationssysteme?

Die Fragen 1.1., 2.1., 2.2. und 2.3. werden aufgrund des Sachzusammenhangs gemeinsam beantwortet:

Die Bayerische Polizei trifft eine Vielzahl von Maßnahmen, um Missbrauch vorzubeugen und sicherzustellen, dass auf die polizeilichen Datenbestände nur innerhalb der gesetzlichen Vorgaben zugegriffen wird.

Jede Polizeidienststelle hat beim Einsatz von Informations- und Kommunikationstechnik dafür Sorge zu tragen, dass den Anforderungen an Datensicherheit und Datenschutz nach Maßgabe der einschlägigen gesetzlichen Vorgaben in der jeweils geltenden Fassung in vollem Umfang entsprochen wird. Über deren Inhalt ist jeder Anwender im Rahmen einer jährlichen Belehrung zu unterrichten.

Spezielle Rechte- und Rollenkonzepte legen fest, welcher Personenkreis Zugang zu den jeweiligen Datenbeständen erhält. In der Folge wird auch eine entsprechende technische Umsetzung, u. a. über eine zentrale Beschäftigtendatenbank veranlasst. Für die zentralen Verfahren sind demnach entsprechende Authentifizierungsverfahren für die eindeutige Identifikation der Nutzer als auch Autorisierungsverfahren für die Zuweisung und Überprüfung der Rechte implementiert. Dies gilt auch für die Rechtevergabe selbst.

Im Rahmen der Datenverarbeitung besteht unter anderem die Möglichkeit, Vorgänge für Rechercheanfragen durch die Vergabe eines sog. „Satzschutzvermerks“ zu sperren. Hierdurch ist sowohl die Sicht als auch der Zugriff auf den jeweiligen Vorgang von vornherein ausgeschlossen, sofern einzelne Beamte hierfür nicht gesondert berechtigt wurden.

Technisch und organisatorisch ist somit sichergestellt, dass sowohl Beamte als auch Polizeibeschäftigte (mit entsprechender sicherheitsrechtlicher Überprüfung und mit der Verpflichtung zur Geheimhaltung) nur zu den Datenbeständen Zugang haben, welche sie zur Erfüllung ihrer Aufgaben benötigen.

zu 1.2.
Gibt es bei allen bayerischen Polizeibehörden eine vollständige Protokollierung aller getätigten Abfragen, Änderungen und weiterer Verarbeitungsvorgänge?

Nach den gesetzlichen Erfordernissen des Art. 63 Abs. 2 Satz 1 Polizeiaufgabengesetz (PAG) bzw. Art. 46 PAG (alte Fassung) i. V. m. Art. 94a PAG werden Verarbeitungstätigkeiten von polizeilichen Verfahren protokolliert. Für jeden Datenabruf besteht eine eindeutige Zuordnung zu den mitprotokollierten Benutzer- und Clientdaten.

Diese Protokolldateien ermöglichen über die stichprobenartige Kontrolle (vgl. 1.3.) hinaus eine zielgerichtete Überprüfung sämtlicher getätigter Zugriffe für den Fall, dass Anhaltspunkte für einen Missbrauch vorliegen.

Für den erstmaligen Einsatz automatisierter Verfahren ist darüber hinaus nach Art. 64 PAG eine sog. Errichtungsanordnung, die unter Zustimmungsvorbehalt des Staatsministeriums des Innern, für Sport und Integration steht, zu erstellen. In dieser Errichtungsanordnung sind u. a. die speichernde Stelle, die Bezeichnung und der Zweck der Datei, der betroffene Personenkreis, wie auch die Überprüfungsfristen und Speicherdauer festzulegen.

zu 1.3.
Gibt es in den verschiedenen Organisationseinheiten auf dem Zufallsprinzip beruhende, automatisierte Stichprobenkontrollen zur Verhinderung unberechtigter Zugriffe? (Bitte mit genauen Angaben zu Art und Häufigkeit der Kontrollen)

Zur Gewährleistung der Einhaltung datenschutzrechtlicher Erfordernisse wurde beim Datenabgleich in den Informationssystemen der Bayerischen Polizei ab dem 01.07.1998 eine bayernweit einheitliche automatisierte Stichprobenkontrolle (sog. „Anlassunabhängige Auswahlprotokollierung“) implementiert. Damit werden täglich technisch automatisiert Abfragen zufällig ausgewählt. Diese sind sodann vom zuständigen Dienststellenleiter zu überprüfen. Sollten sich Anhaltspunkte für eine missbräuchliche Abfrage des Datenbestands ergeben, sind die im Rahmen der Dienst- und Fachaufsicht geeigneten Maßnahmen einzuleiten.

Aktuell wurde die Erhöhung der Anzahl an automatisierten Stichprobenkontrollen im Rahmen der „Anlassunabhängigen Auswahlprotokollierung“ von zehn auf 100 Stichprobenkontrollen pro Tag technisch implementiert. Die Einführung der Stichprobenkontrolle für weitere Verfahren und Datenbanken wird derzeit geprüft.

zu 4.3.
Wie wird gewährleistet, dass über die eigene persönliche Kennung bzw. das eigene persönliche Password keine anderen Benutzer einen Systemzugang erhalten?

Nach gültiger Regelungslage wird jeder Nutzer jährlich unterschriftlich über den Umgang mit dienstlichen IuK-Geräten belehrt. Hierzu zählt unter anderem die Passwort-Richtlinie, welche die Ausgestaltung der persönlichen Kennung nach den etablierten IT-Sicherheitsrichtlinien sowie eine verpflichtende Änderung der Kennung nach bestimmten Zeitintervallen regelt.

Zudem ist der Bildschirm auch beim kurzfristigen Verlassen des Arbeitsplatzes manuell zu sperren. Eine automatische Sperrung erfolgt nach einem festgelegten Zeitintervall der Inaktivität des Nutzers.

Darüber hinaus wurde durch das Informationssicherheitsmanagement der Bayerischen Polizei das elektronische Lernprogramm „Grundlagen der IT-Sicherheit“ initiiert, welches seit dem Jahr 2018 verpflichtend durch alle Polizeibeschäftigten zu absolvieren ist. Im Rahmen des Lernprogramms erfolgt unter anderem die Sensibilisierung für die Grundlagen der Informationssicherheit, insbesondere auch zu den Themenfeldern Vertraulichkeit und Integrität sowie dem Umgang mit Passwörtern und der Erstellung sicherer Passwörter.

zu 3.1.
Wie viele unrechtmäßige Datenabfragen durch Mitarbeiterinnen und Mitarbeiter bayerischer Polizeibehörden wurden im Zeitraum 2017 bis erstes Halbjahr 2020 festgestellt? (Bitte mit genauer Zuordnung zur betroffenen Polizeibehörde und Kalenderjahr)

Bei den genannten Zahlen handelt es sich um die eingeleiteten Ordnungswidrigkeitsverfahren gegen eine oder einen Beschäftigten. Innerhalb der jeweiligen Verfahren tätigte die- oder derjenige meist mehrere unberechtigte Abfragen, sodass jeweils tatmehrheitliche Verstöße innerhalb eines Ordnungswidrigkeitsverfahrens geahndet wurden. Daher können die Verfahren auch Abfragen aus vorherigen Jahren, z. B. 2016, enthalten. Als Zeitpunkt wurde die Einleitung des Verfahrens festgelegt. Es können daher auch Verfahren beinhaltet sein, die sich letztlich nicht bestätigten oder noch laufen.

Verband	2017	2018	2019	2020 (zum Stichtag 30.06.2020)
PP OBN	3	2	5	3
PP OBS	0	5	3	4
PP M	14	4	15	3
PP NB	2	7	4	1
PP OPf	0	1	1	1
PP OFr	1	4	0	1
PP MFr	20	9	1	2
PP UFr	7	3	1	1
PP SWN	0	3	9	1
PP SWS	9	5	4	6
BPP	1	5	2	1
BLKA	4	3	1	0
PVA	0	0	0	0
Gesamt	61	51	46	24

zu 3.2.

Welche Datenbanken waren von den missbräuchlichen Datenabfragen betroffen?

Die Abfragen erfolgten in den folgenden Datenbanken:
Informationssystem der Polizei (INPOL), Einwohnermeldedatei (EWO), Integrationsverfahren Polizei (IGVP), Rechercheanwendung zu IGVP (IGWeb), Vorgangsverwaltung (VVW), Kraftfahrtbundesamt – Abfrage von Fahrerlaubniseinschränkungen (KBA-FAER), Zentrales Verkehrs-Informationssystem (ZEVIS), Programm

zur Bearbeitung von Verkehrsordnungswidrigkeiten in Bayern (ProVi Bayern), Dateien der Landeshauptstadt München (SMU), Ausländerzentralregister (AZR) und Schengener Informationssystem (SIS).

zu 3.3.
In wie vielen Fällen missbräuchlicher Datenabfragen erfolgte eine Weiterleitung der abgefragten Daten innerhalb der Behörde oder an externe Personen?

In 19 Fällen erfolgte eine Weiterleitung der abgefragten Daten innerhalb der Behörde oder an externe Personen. Sofern personenbezogene Daten aus polizeilichen Recherche- und Auskunftssystemen unbefugt an Personen außerhalb der Behörde übermittelt werden und somit der Anfangsverdacht von Straftaten, insbesondere des Vergehens nach § 353b StGB – Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht – im Raum stehen, werden die entsprechenden Ermittlungsverfahren beim Bayerischen Landeskriminalamt, Dezernat 13, geführt.

zu 4.1.
Welche disziplinarischen und arbeitsrechtlichen Konsequenzen wurden in den betroffenen bayerischen Polizeidienststellen aus den festgestellten unrechtmäßigen Datenabfragen gezogen?

Durch unberechtigte Datenabfragen verletzt eine Beamtin oder ein Beamter die Pflichten, dienstliche Anordnungen und allgemeine Richtlinien zu befolgen (§ 35 Satz 2 Beamtenstatusgesetz – BeamtStG), sich seinem Beruf entsprechend achtungs- und vertrauenswürdig zu verhalten (§ 34 Satz 3 BeamtStG), sowie die Gesetze zu beachten (Art. 20 Abs. 3 GG i. V. m. Art. 23 Abs. 1 Nr. 1 Buchstabe c Bayerisches Datenschutzgesetz – BayDSG).

Die Disziplinarmaßnahme gem. Art. 14 Abs. 1 Satz 2 Bayerisches Disziplinargesetz (BayDG) ist insbesondere nach der Schwere des Dienstvergehens, der Beeinträchtigung des Vertrauens des Dienstherrn oder der Allgemeinheit, dem Persönlichkeitsbild und dem bisherigen dienstlichen Verhalten zu bemessen. Eine Regelmaßnahme existiert nicht, da immer die Umstände des Einzelfalls in die Entscheidung einzubeziehen sind. Sofern kein über die Datenabfrage hinausgehender Vorwurf zu erkennen ist, wäre je nach Einzelfall in der Regel eine Geldbuße zu

verhängen. Diese Maßnahmen dürfen jedoch nach Art. 15 Abs. 1 BayDG nicht mehr verhängt werden, wenn im Ordnungswidrigkeitsverfahren bereits eine Geldbuße verhängt wurde. Gegen Beschäftigte, die unrechtmäßige Datenabfragen tätigen, werden grundsätzlich Ordnungswidrigkeitsverfahren nach Art. 23 Abs. 1 Nr. 1 Buchstabe c BayDSG i. V. m. § 17 Gesetz über Ordnungswidrigkeiten (OWiG) eingeleitet. Sofern kein über die Datenabfrage hinausgehender Vorwurf zu erkennen ist, greift das genannte Maßnahmenverbot des Art. 15 Abs. 1 Nr. 1 BayDG, wenn im Ordnungswidrigkeitsverfahren eine Geldbuße festgelegt wurde. Das Verhalten wird daher in der Regel im Nachgang des Ordnungswidrigkeitsverfahrens zusätzlich schriftlich missbilligt. Wurden die abgefragten Daten an Dritte außerhalb des Polizeibereichs weitergegeben (vgl. § 353b StGB), ist regelmäßig die Einleitung eines förmlichen Disziplinarverfahrens mit dem Ziel der Gehaltskürzung zu prüfen.

Tarifbeschäftigte verstoßen durch unerlaubte Datenabfragen dagegen gegen ihre arbeitsvertraglichen Nebenpflichten, über welche sie beim Abschluss des Arbeitsvertrags schriftlich belehrt werden. Auf die arbeitsvertraglichen Nebenpflichten müssen Arbeitnehmerinnen und Arbeitnehmer über die Hauptleistungspflicht hinaus Rücksicht nehmen. Je nach Anzahl und Schwere der unerlaubten Datenabfragen werden die Arbeitnehmer belehrt, abgemahnt und im schlimmsten Fall erfolgt eine Kündigung des Arbeitsverhältnisses.

zu 4.2.
Wurden bestehende Kontrollmechanismen aufgrund festgestellter Missbräuche bei den Datenabfragen verändert oder verschärft?

Eine Verschärfung von bestehenden Kontrollmechanismen aufgrund festgestellter Missbräuche innerhalb der Bayerischen Polizei erfolgte nicht.

zu 5.1.
Wie viele unrechtmäßige Datenabfragen durch Mitarbeiterinnen und Mitarbeiter des bayerischen Landeskriminalamtes wurden im Zeitraum 2017 bis erstes Halbjahr 2020 festgestellt? (Bitte mit genauer Aufschlüsselung nach Kalenderjahr und betroffenen Datenbanken)

Beim Bayerischen Landeskriminalamt wurden im Zeitraum 2017 bis zum ersten Halbjahr 2020 insgesamt acht Ordnungswidrigkeitsverfahren eingeleitet. Auf die zur Erhebung der Zahlen zugrunde gelegten Parameter wird auf Ziffer 3.1. verwiesen.

Verband	2017	2018	2019	2020 (zum Stichtag 30.06.2020)
BLKA	4	3	1	0

zu 5.2.
Inwiefern erfolgte eine Weiterleitung der Daten innerhalb der Behörde oder an externe Personen?

In einem Fall wurden die Daten einer verdächtigen Person im Rahmen einer Ermittlung in eigener Sache recherchiert (vgl. Ziffer 6.1) und anschließend an die zuständige Polizeidienststelle weitergeleitet.

zu 5.3.
Welche disziplinarischen und arbeitsrechtlichen Konsequenzen wurden aus den festgestellten unrechtmäßigen Datenabfragen beim Landeskriminalamt gezogen?

Siehe Antwort zu Frage 4.1.

zu 6.1.
Welche Motive für die unrechtmäßigen Datenabfragen konnten ermittelt werden?

In den meisten Fällen waren private Motive (Abfrage der eigenen Person, privater Kontakt, eigener Mieter, Vereinskameraden, Kolleginnen und Kollegen, laufende Strafverfahren etc.) die Ursache für die unrechtmäßigen Datenabfragen.

Daneben erfolgten auch Abfragen im Rahmen von Ermittlungen in eigener Sache. In diesen Fällen wurde nicht beachtet, dass bei Ermittlungen in eigener Sache der Vorgang nicht durch den betreffenden Beamten/die betroffene Beamtin selbst aufgenommen werden darf.

zu 6.2.
Welche Rolle spielen private Motive und Interessen bei den missbräuchlichen Datenabfragen?

Wie unter Ziffer 6.1. dargestellt, waren private Motive der nahezu ausschließliche Grund für unzulässige Datenabfragen.

zu 6.3.
Konnten auch missbräuchliche Datenabfragen aus politischen Motiven festgestellt werden?

Missbräuchliche Datenabfragen aus politischen Motiven konnten nicht festgestellt werden.

zu 7.1.
An welchen gemeinsamen Datenbanken mit Sicherheitsbehörden des Bundes beteiligen sich bayerische Sicherheitsbehörden?

Die Bayerische Polizei nimmt gem. § 29 Abs. 3 Nr. 1 Bundeskriminalamtgesetz (BKAG) am Informationssystem der Polizei (INPOL), bei dem es sich um ein durch das Bundeskriminalamt bereitgestelltes Verbundsystem von Bund und Ländern handelt, teil. Zudem beteiligt sich die Bayerische Polizei am Polizeilichen Informations- und Analyseverbund (PIAV) in den Phänomenbereichen Waffen-/Sprengstoffkriminalität, Gewaltdelikte und Gemeingefährliche Straftaten, Rauschgift, Eigentumskriminalität/Vermögensdelikte, Cybercrime, Sexualdelikte, Dokumentenkriminalität, Schleusung/Menschenhandel und Ausbeutung sowie der Antiterrordatei (ATD).

Das Bayerische Landesamt für Verfassungsschutz (BayLfV) nimmt gemäß § 6 Abs. 2 Satz 1 Bundesverfassungsschutzgesetz (BVerfSchG) an der Verbunddatei NADIS-WN, sowie der Antiterrordatei (ATD) und der Rechtsextremismus-Datei (RED) entsprechend den Regelungen des Antiterrordateigesetzes (ATDG) und des Rechtsextremismus-Datei-Gesetzes (RED-G) teil.

zu 7.2.
An welchen gemeinsamen Datenbanken mit ausländischen Sicherheitsbehörden beteiligen sich bayerische Sicherheitsbehörden?

Die Bayerische Polizei beteiligt sich am Schengener Informationssystem (SIS), dem Visa Informationssystem (VIS), dem Europol Informationssystem (EIS), dem Fingerabdruck-Identifizierungssystem (European Dactyloskopie – Eurodac), sowie dem Europäischen Grenzüberwachungssystem (European Border Surveillance System – EUROSUR). Künftig ist eine Beteiligung am Ein-/Ausreisesystem (Entry/Exit-System – EES) sowie dem Europäischen Reiseinformations- und -genehmigungssystem (European Travel Information and Authorisation System – ETIAS) vorgesehen.

Die Befugnis zur Teilnahme an gemeinsamen Dateien mit ausländischen Nachrichtendiensten besteht gem. § 22c BVerfSchG nur für das Bundesamt für Verfassungsschutz (BfV).

zu 8.1.
Welche Sicherungsmaßnahmen gegen unrechtmäßige Datenabfragen gibt es beim bayerischen Landesamt für Verfassungsschutz?

Es bestehen umfangreiche gesetzliche und behördliche Sicherungsmechanismen.

Für die einzelnen Abfragen existieren gesetzliche Protokollierungs- und Aufzeichnungspflichten sowohl für die datei-/registerführende als auch für die abfragende Stelle (vgl. z. B. § 6 Abs. 3 BVerfSchG, § 10 Abs. 1 RED-G, § 9 Abs. 1 ATDG, § 40 Bundesmeldegesetz (BMG), §§ 1 Abs. 1, 20 Abs. 2, 22 Absatz 2 Satz 2 des Gesetzes über das Ausländerzentralregister (AZRG), §§ 12, 20 Waffenregistergesetz (WaffRG)).

Die Abfragen können in der Regel nur unter Nutzung einer persönlichen Kennung durchgeführt werden (so z. B. bei NADIS-WN, ATD, RED).

Zudem sind für Abfragen im Verbundsystem NADIS-WN die Angaben eines Abfragegrundes und eines Aktenzeichens zwingend erforderlich. Die in NADIS implementierten externen Behördenanfragen (z. B. bei Bundeskriminalamt (BKA), Bundeszentralregister (BZR) und zukünftig auch Waffenregister und Ausländerzentralregister (AZR)) sind von den NADIS-Sicherungsmechanismen umfasst. Die Protokollierung der Zugriffe erfolgt beim BfV.

In den für Ermittlungen zuständigen Organisationseinheiten des BayLfV werden zu Dokumentationszwecken zusätzlich umfangreiche Aufzeichnungen zu den abgefragten Datenbanken (z. B. Melderegister) angefertigt (vgl. Art. 7 Bayerisches Verfassungsschutzgesetz (BayVSG)). Für den erstmaligen Einsatz automatisierter Dateien sind darüber hinaus nach Art. 22 BayVSG unter anderem Festlegungen zur Protokollierung in einer sog. Errichtungsanordnung zu treffen. Über die Errichtungsanordnungen ist ein Verzeichnis zu führen.

Eine weitere Kontrolle findet im Wege der Dienstaufsicht durch die jeweiligen Vorgesetzten statt. Darüber hinaus werden die Mitarbeitenden (z. B. im Einführungslehrgang sowie in weiterführenden Lehrgängen) regelmäßig hinsichtlich der dienst- und arbeitsrechtlichen sowie straf- und ordnungswidrigkeitsrechtlichen Konsequenzen etwaiger nicht dienstlich veranlasster Abfragen sensibilisiert.

zu 8.2.
Wie häufig kam es im Zeitraum 2017 bis erstes Halbjahr 2020 zu unberechtigten Datenabfragen durch Mitarbeiterinnen und Mitarbeiter des bayerischen Landesamtes für Verfassungsschutz?

zu 8.3.
Welche disziplinarischen und arbeitsrechtlichen Konsequenzen wurden aus festgestellten missbräuchlichen Datenabfragen im Bereich des Landesamtes für Verfassungsschutz gezogen?

Die Fragen 8.2. und 8.3. werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Im Anfragezeitraum wurden keine unberechtigten Datenabfragen beim Bayerischen Landesamt für Verfassungsschutz festgestellt.

zu 7.3.
Welche Sicherungsmaßnahmen gegen unrechtmäßige Datenabfragen existieren bei den internationalen Datenbanken und den Datenbanken des Bundes?

Zu den Sicherungsmaßnahmen der jeweiligen Datenbanken selbst kann keine Aussage getroffen werden, da die bayerischen Sicherheitsbehörden diese Datenbanken weder errichtet haben noch betreiben.

Für die Zugriffe von Beschäftigten der bayerischen Sicherheitsbehörden verweisen wir in diesem Zusammenhang auf die Beantwortung der Fragen zu 1.1., 2.1., 2.2., 2.3. sowie 8.1.

Mit freundlichen Grüßen

gez. Gerhard Eck
Staatssekretär