Deutscher Bundestag **Drucksache 19/22897**

19. Wahlperiode 29.09.2020

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/21989 –

Kontrolle unrechtmäßiger Datenbankabfragen durch Sicherheitsbehörden des Bundes

Vorbemerkung der Fragesteller

Polizeiliche Verbunddateien enthalten eine Vielzahl personenbezogener Daten über Bürgerinnen und Bürger, deren unrechtmäßiger Abruf durch die im polizeilichen Informationssystem beteiligten Behörden nach Auffassung der Fragestellerinnen und Fragesteller nicht hingenommen werden darf. Angesichts von Meldungen, dass es insbesondere im Land Hessen zu mehreren solcher unberechtigter Abfragen gekommen ist (https://www.tagesschau.de/investigativ/swr/polizei-hessen-109.html), das Problem aber auch bundesweit auftritt (https://www.tagesschau.de/inland/datenabfragen-polizei-101.html), halten die Fragestellerinnen und Fragesteller es für geboten, auch die Kontrollverfahren bei Sicherheitsbehörden des Bundes zu hinterfragen und ggf. zu überarbeiten. Denn es gilt zu verhindern, dass beispielsweise Rechtsextreme bei der Bundespolizei oder dem Bundeskriminalamt (BKA) Daten über politische Gegnerinnen und Gegner einsehen und ggf. weiterleiten können. Auch sonstige, aus privaten Motiven gespeiste unrechtmäßige Datenabfragen müssen nach Ansicht der Fragestellerinnen und Fragesteller nach Möglichkeit verhindert werden.

Teil des Problems ist nach Auffassung der Fragestellerinnen und Fragesteller die unzulängliche Prüf- bzw. Aussonderungspraxis der Daten insbesondere in den Staatsschutzdateien (vgl. Kritik der früheren Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, https://www.tagesschau.de/investigativ/g20-presse-101.html, außerdem die Erläuterung der Bundesregierung, Grund für die Mängel in der Dateipflege sei ein „uneinheitliches Meldeverhalten der Justizbehörden“, Antwort zu Frage 5 auf Bundestagsdrucksache 18/13653). Es liegt nach Ansicht der Fragestellerinnen und Fragesteller auf der Hand, dass gerade diese Datenbänke mit Informationen zu (tatsächlichen oder nur vermeintlichen) politisch motivierten Straftätern für Rechtsextreme besonders interessant sind; ein Weniger an Datenspeicherung wäre hier ein Mehr an Sicherheit.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 28. September 2020 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

In ihrer Antwort auf die Schriftliche Frage der Abgeordneten Ulla Jelpke auf Bundestagsdrucksache 19/21517 stellte die Bundesregierung einige exemplarische Kontrollmechanismen beim Bundeskriminalamt (BKA) und der Bundespolizei vor, ohne diese aber vollständig und im Detail zu erläutern. Die Fragestellerinnen und Fragesteller begehren diesbezüglich mehr Auskünfte.

Vorbemerkung der Bundesregierung

Die Antwort zu den Fragen 15 und 20 kann in Teilen nicht offen erfolgen. Die Einstufung der Antwort auf die Frage als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ ist im vorliegenden Fall im Hinblick auf Gründe des Staatswohls erforderlich. Nach der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern, für Bau und Heimat zum materiellen und organisatorischen Schutz von Verschlusssachen (Verschlusssachenanweisung, VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Fragen würde Informationen zu den Sicherungsmechanismen bei Datenbankabfragen des Bundesnachrichtendienstes (BND) einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Eine solche Veröffentlichung von Einzelheiten ist daher geeignet, zu einer wesentlichen Verschlechterung der dem BND zur Verfügung stehenden Möglichkeiten der Informationsgewinnung zu führen. Diese Informationen werden daher als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

1. Welche bundeseinheitlichen Kontrollmechanismen gibt es zur Erfassung bzw. Verhinderung von unrechtmäßigen Datenabfragen aus dem polizeilichen Informationssystem (bitte vollständig darlegen), und inwiefern werden diese auch von Sicherheitsbehörden des Bundes vollumfänglich angewandt?

Als Kontrollmechanismus für die polizeilichen Verbund- und Zentraldateien dient die vollständige Protokollierung aller getätigten Abfragen, Änderungen oder weiterer Verarbeitungsvorgänge gemäß den Vorgaben des § 76 des Bundesdatenschutzgesetzes (BDSG).

Hinsichtlich des Zugriffs auf gespeicherte Dateien im polizeilichen Informationssystem existieren bundesweit Regelungen zu detaillierten Zugriffsberechtigungen, die auf den konkreten Aufgaben und Zuständigkeiten des jeweils einzelnen Sachbearbeiters basieren.

In der Bundespolizei ist der Zugriff auf Datei- und Informationssysteme, die personenbezogene Daten enthalten, durch ein detailliertes Rechte- und Rollenkonzept geregelt.

Darüber hinaus erfolgt eine systemseitige Protokollierung nach datenschutzrechtlichen Vorgaben und dem „Mindeststandard des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Protokollierung und Detektion von Cyber-Angriffen“.

2. Was ist mit der in der Antwort auf die erwähnte Schriftliche Frage (siehe Vorbemerkung der Fragesteller) genannten „Vielzahl polizeilicher Daten-/Datenverarbeitungen“, für die eine auf dem Zufallsprinzip beruhende Stichprobenkontrolle beim BKA eingeführt wurde, gemeint (bitte vollständig ausführen)?

   Warum ist diese Kontrollmethode nicht für sämtliche polizeiliche Daten bzw. Datenverarbeitungen etabliert?

Neben INPOL als zentrales Fahndungs- und Auskunftssystem der deutschen Polizeien unterliegen auch sämtliche INPOL-Fall-Dateien (Fallbearbeitungs- und Analysesystem mit verbundrelevanten Daten), alle auf b-case (Fallbearbeitungssystem des Bundeskriminalamtes – BKA und der Bundespolizei) basierenden Zentral- und Amtsdateien, das einheitliche Fallbearbeitungssystem (eFBS) und das BKA eigene Vorgangsbearbeitungssystem (VBS) dieser Stichprobenkontrolle. Die Kontrollmethode wurde überall dort eingeführt, wo es auf Grund der bestehenden technischen Systeme möglich war.

3. Wie genau funktioniert die auf dem Zufallsprinzip beruhende automatisierte Stichprobenkontrolle?

Nach dem Zufallsprinzip wird rechnerisch eine von tausend Abfragen mit einem sogenannten Sperrbildschirm belegt. Das Ergebnis der Abfrage wird in diesen Fällen erst nach Eintragung des Abfragegrunds angezeigt.

Wird der Sperrbildschirm aktiv abgebrochen oder nach gewisser Zeit automatisch geschlossen, erhält der behördliche Datenschutzbeauftragte des BKA eine entsprechende Mitteilung und fordert den Abfragegrund sowie den Grund für den Abbruch/Zeitablauf nach.

a) Wie viele Stichproben werden auf je 100 oder 1 000 Datenabfragen durchgeführt?

Aktuell wird eine Stichprobe auf eintausend Dateiabfragen erhoben.

b) Inwiefern kann hierbei erkannt werden, ob ein Datenabruf unrechtmäßig war?

Der Abfragende muss bei der Stichprobenkontrolle den Grund für die Abfrage angeben. Dieser wird vom behördlichen Datenschutzbeauftragten und seinen Mitarbeitern auf Plausibilität geprüft.

c) Von wem wird, wie die Bundesregierung in ihrer Antwort auf die Schriftliche Frage ausführt, diesem Kontrollmechanismus eine „deutlich abschreckende Wirkung beigemessen“, und woraus resultiert diese Bewertung?

Grundlage ist die Einschätzung der Amtsleitung des BKA und des behördlichen Datenschutzbeauftragten des BKA. Die abschreckende Wirkung beruht darauf, dass die Sachbearbeiter im BKA die Zufallsstichprobe in ihrem Arbeitsalltag konkret erleben. Darüber ermöglicht es die vollständige Protokollierung aller Verarbeitungsvorgänge gemäß den Vorgaben des § 76 BDSG, anlassbezogen und bei Vorliegen der rechtlichen Voraussetzungen nachträglich die Rechtmäßigkeit der getätigten Abfragen zu prüfen.

4. Wie häufig kam es nach Kenntnis der Bundesregierung und gegebenenfalls hochgerechnet aus den Stichproben des Kontrollmechanismus in den Jahren 2017, 2018, 2019 und im ersten Halbjahr 2020 zu unrechtmäßigen Datenabfragen innerhalb des BKA bzw. durch Mitarbeiterinnen und Mitarbeiter des BKA (hier bitte auch die Zentraldateien berücksichtigen)?

Für das Jahr 2017 liegt keine Statistik vor.

Im Jahr 2018 und im ersten Halbjahr 2020 konnten keine missbräuchlichen Datenabfragen festgestellt werden.

Im Jahr 2019 kam es zu zwei missbräuchlichen Datenabfragen.

a) Welche Art von Daten sowie welche Datenbanken waren davon betroffen (bitte so vollständig wie möglich angeben)?

Betroffen waren in einem Fall die Verbunddatei INPOL, in dem zweiten Fall das Einwohnermelderegister Baden-Württemberg.

b) Inwiefern konnte festgestellt werden, ob die unrechtmäßig abgefragten Daten innerhalb der Behörde oder an externe Personen weitergeleitet wurden, und falls letzteres der Fall war, welche Angaben kann die Bundesregierung zu diesen externen Personen machen?

In einem Fall stand als Ergebnis der internen Ermittlungen fest, dass der Hintergrund der Abfrage die private Neugier des/der Abfragenden war und keine Weitergabe erfolgte.

Im zweiten Fall erfolgte die Abfrage im Interesse eines Bekannten des/der Abfragenden an Speicherungen zu seiner Person, die durch den/die Abfragende/n dann auch an ihn weitergeben wurden.

c) Inwiefern konnten die hierfür verantwortlichen Mitarbeiter und Mitarbeiterinnen namentlich zugeordnet werden?

Auf die Antwort zu Frage 4b wird verwiesen.

d) Welche Motive für die unrechtmäßigen Datenabfragen konnten ermittelt werden?

Auf die Antwort zu Frage 4b wird verwiesen.

e) Welche disziplinarischen oder rechtlichen Konsequenzen wurden gezogen?

In einem Fall wurde ein Disziplinarverfahren eingeleitet, das zur Verhängung einer Geldbuße in Höhe von 600 Euro als Disziplinarmaßnahme führte.

Der andere Fall führte zu einem arbeitsrechtlichen Verfahren, das mit der fristlosen Entlassung endete.

f) Welche weiteren Schlussfolgerungen wurden aus den Vorfällen gezogen?

Beide Fälle haben gezeigt, dass der Kontrollmechanismus funktioniert.

5. Wann wurden die bestehenden Kontrollmechanismen beim BKA seit 2017 auf ihre Wirksamkeit überprüft und angepasst, und was waren die jeweiligen Anlässe, aus denen heraus eine Anpassung für notwendig gehalten wurde?

Die Überprüfung fand anlassunabhängig statt. Die Rate für die gezogenen Stichproben wurde jedoch auch aufgrund des Bekanntwerdens unrechtmäßig erfolgter Abfragen in einzelnen Bundesländern erhöht.

6. Wie ist die Aussage der Bundesregierung in der Antwort auf die Schriftliche Frage zu verstehen, die „bestehenden technischen Sicherungsmechanismen zur Verhinderung besagter unberechtigter Zugriffe sind bei der Bundespolizei vollumfänglich vorhanden“?

   Welche Sicherungsmechanismen genau werden angewandt (bitte vollständig ausführen)?

Für die Sicherstellung der Verhinderung von unberechtigten Zugriffen auf die Verbunddaten des polizeilichen Informationsverbundes hat die Bundespolizei ein mehrstufiges dediziertes Rollen- und Rechtekonzept umgesetzt, bei dem die Mitarbeiter individuell und ausschließlich mit Bezug zur jeweiligen Aufgabenwahrnehmung Zugriffsrechte auf notwendige Informationen erhalten. Alle Zugriffe werden mindestens entsprechend des „Mindeststandards des BSI zur Protokollierung und Detektion von Cyber-Angriffen“ protokolliert und ein unberechtigter Zugriffsversuch entsprechend den Schutzmaßnahmen verhindert bzw. detektiert.

Im Übrigen ist es nach der „Dienstanweisung für die Nutzung der Informations- und Kommunikationstechnik“ unzulässig, anderen Benutzern den Systemzugang mit dem eigenen persönlichen Passwort bzw. der eigenen persönlichen Kennung zu ermöglichen. Sämtliche protokollierte Aktivitäten werden dem jeweiligen Inhaber der persönlichen Kennung zugerechnet.

Für verschiedene IT-Anwendungen/Endgeräte sind unterschiedliche Passwörter zu verwenden. Das Ausprobieren, Ausforschen oder die Nutzung fremder Identifikationsmittel (z. B. fremde Benutzerkennungen) und sonstiger Authentifizierungshilfsmittel (z. B. fremde Passwörter) sind verboten. Das Passwort ist unverzüglich zu ändern, sofern zu vermuten ist, dass das Passwort kompromittiert worden ist. Wurde das Passwort vergessen, ist der IKT-ServiceDesk persönlich zu kontaktieren. Hierüber sind die Beamtinnen und Beamten regelmäßig zu belehren.

7. Wird auch bei der Bundespolizei eine Stichprobenkontrolle zu Datenabfragen durchgeführt, und wenn nein, warum nicht, und wenn ja,

   a) wie genau funktioniert diese Stichprobenkontrolle,

   b) wie viele Stichproben werden auf je 100 oder 1000 Datenabfragen durchgeführt,

   c) inwiefern kann hierbei erkannt werden, ob ein Datenabruf unrechtmäßig war?

Fachlich sind in den Fall- und Vorgangsbearbeitungssystemen sowie im Fahndungs- und Auskunftssystem keine Stichprobenkontrollen vorgesehen. Gleichwohl erfolgen Kontrollen durch den behördlichen Datenschutzbeauftragten der Bundespolizei im Rahmen seiner gesetzlich geregelten Aufgabenwahrnehmung.

8. Wie häufig kam es 2017, 2018, 2019 und im ersten Halbjahr 2020 zu unrechtmäßigen Datenabfragen durch die Bundespolizei bzw. Mitarbeiterinnen und Mitarbeiter der Bundespolizei?

- Jahr 2017: unberechtigte Datenabfragen in vier Fällen.
- Jahr 2018: unberechtigte Datenabfragen in 17 Fällen.
- Jahr 2019: unberechtigte Datenabfragen in sieben Fällen.
- Jahr 2020: unberechtigte Datenabfragen in drei Fällen.

a) Welche Art von Daten sowie welche Datenbanken waren davon betroffen (bitte so vollständig wie möglich angeben)?

- Jahr 2017: ZEVIS (zentrales Verkehrsinformationssystem), INPOL, EWO (Meldedateien der Einwohnermeldeämter) – Halterdaten, Meldedaten, Abfragen im Fahndungsbestand
- Jahr 2018: INPOL, EWO – Abfragen im Fahndungsbestand, Meldedaten
- Jahr 2019: INPOL, EWO, AZR (Ausländerzentralregister), ZEVIS – Abfragen im Fahndungsbestand, Meldedaten, Abfrage von KFZ-Kennzeichen
- Jahr 2020: INPOL, ZEVIS – Abfragen im Fahndungsbestand, Personendaten, Meldedaten

b) Inwiefern konnte festgestellt werden, ob die unrechtmäßig abgefragten Daten innerhalb der Behörde oder an externe Personen weitergeleitet wurden, und falls letzteres der Fall ist, welche Angaben kann die Bundesregierung zu diesen Personen machen?

- Jahr 2017: In zwei Fällen erfolgte keine Weiterleitung der Daten. In einem Fall erfolgte eine interne Weiterleitung innerhalb der Behörde. In einem Fall erfolgte die Datenweiterleitung an eine externe Person; die Person ist der Bundespolizei bekannt.
- Jahr 2018: Es erfolgte in zwei Fällen die Weiterleitung der Daten an eine externe Person; diese sind der Bundespolizei namentlich bekannt.
- Jahr 2019: Es erfolgte in einem Fall eine Weiterleitung der Daten innerhalb der Behörde. In einem Fall erfolgte die Weiterleitung der Daten an eine externe Person; die Person ist der Bundespolizei bekannt.
- Jahr 2020: In zwei Fällen erfolgte die Weiterleitung der Daten an eine externe Person; die Person ist der Bundespolizei bekannt.

c) Inwiefern konnten die hierfür verantwortlichen Mitarbeiterinnen und Mitarbeiter namentlich zugeordnet werden?

- In allen Fällen der Jahre 2017 bis 2020 konnten die hierfür verantwortlichen Mitarbeiterinnen und Mitarbeiter namentlich zugeordnet werden.

d) Welche Motive für die unrechtmäßigen Datenabfragen konnten ermittelt werden?

- Jahr 2017: Private Interessen, Gefallen für Bekannte.

- Jahr 2018: Private Interessen, Neugier, Abfrage von Angehörigen, Abfrage von Prominenten aus Showbusiness.
- Jahr 2019: Private Interessen, Neugier, Abfrage von Angehörigen, Abfrage von Prominenten, Abfrage für Kollegen.
- Jahr 2020: Private Interessen, Abfrage von Fahndungstreffern für Bekannte.

e) Welche disziplinarischen oder rechtlichen Konsequenzen wurden gezogen?

- Jahr 2017: In drei Fällen wurden Disziplinarmaßnahmen (Geldbußen) verhängt, in einem Fall erfolgte die Entfernung aus dem Beamtenverhältnis. In zwei Fällen wurden strafrechtliche Ermittlungen geführt.
- Jahr 2018: In sechzehn Fällen wurden Disziplinarmaßnahmen (Verweise, Geldbußen, Kürzung der Dienstbezüge) verhängt. In einem Fall erfolgte die Entlassung aus dem Beamtenverhältnis; in diesem Fall wurden strafrechtliche Ermittlungen geführt.
- Jahr 2019: In einem Fall wurde eine Missbilligung ausgesprochen. In sechs Fällen wurden Disziplinarmaßnahmen (Verweise, Geldbußen) verhängt. In einem Fall wurden strafrechtliche Ermittlungen geführt.
- Jahr 2020: In drei Fällen erfolgte die Entlassung aus dem Beamtenverhältnis. In zwei Fällen wurden strafrechtliche Ermittlungen geführt.

f) Welche weiteren Schlussfolgerungen wurden aus den Vorfällen gezogen?

Es erfolgen mehrfache Sensibilisierungen, Mitarbeiterinformationen zur Prävention und Veröffentlichungen im Intranet.

9. Welche Kontrollmechanismen zur Sicherstellung von unberechtigten Zugriffen auf Dateieinträge in den polizeilichen Verbunddateien gibt es im Bereich der Zollverwaltung (bitte vollständig anführen)?

Der Zugang zu den polizeilichen Verbunddaten wird im Bereich der Zollverwaltung durch technische und organisatorische Maßnahmen geschützt. Der Zugriff auf die Daten erfolgt über persönliche Zugriffskennungen und Passwörter, Sammelkennungen werden nicht verwendet.

Über die Benutzerverwaltung des Fachverfahrens INPOL-Zoll werden die Zugriffrechte der Anwender abhängig von deren Aufgabengebieten festgelegt. Zugangskennungen werden nur vergeben, wenn der Anwender zuvor von seiner vorgesetzten Stelle dazu autorisiert wurde.

Das Fachverfahren INPOL-Zoll protokolliert die Abfragen mit der Kennung des Benutzers, dem Abfragezeitpunkt, den Abfragewerten, dem Veranlasser, dem Abfragegrund, der Trefferanzahl und weitere Angaben. Zusätzlich wird verfahrensseitig nach einer definierten Anzahl von Abfragen eine Zusatzprotokollierung aktiviert, bei der der Abfragende aufgefordert wird, Abfrageanlass und Veranlasser zu nennen. Die Informationen werden nach Ablauf eines Jahres automatisch gelöscht. Die Protokolldaten können durch die Systembetreuung in berechtigten Fällen ausgewertet werden.

Daneben übermittelt der Zollfahndungsdienst (ZFD) entsprechend den Vorgaben des Polizeiverbundes Daten aus dem IT-Verfahren INZOLL in den polizeilichen Informations- und Analyseverbund PIAV. Er ist auch berechtigt, Suchanfragen zu stellen.

Neben dem im IT-Verfahren INZOLL geltenden Sicherheitsmechanismen gibt es, bezogen auf den Datenaustausch mit PIAV, weitere Sicherheitsmechanismen:

- Die Berechtigung zum Datenaustausch zwischen INZOLL und PIAV erfordert ein eigenes Recht, das der jeweiligen Benutzerkennung zugewiesen werden muss.
- Diese Berechtigung beinhaltet keinen Zugriff auf sämtliche, sondern nur auf die fachlich für den Teilnehmer notwendigen Deliktsbereiche des PIAV.
- Die Übermittlungen und Suchanfragen werden entsprechend den gesetzlichen Regelungen im IT-Verfahren INZOLL protokolliert und stehen als Protokolldaten den im Gesetz berechtigten Stellen zur Auswertung zur Verfügung.

10. Wird auch bei der Zollverwaltung eine Stichprobenkontrolle zu Datenabfragen durchgeführt, und wenn nein, warum nicht, und wenn ja,

    a) wie genau funktioniert diese Stichprobenkontrolle,

    b) wie viele Stichproben werden auf je 100 oder 1000 Datenabfragen durchgeführt,

    c) inwiefern kann hierbei erkannt werden, ob ein Datenabruf unrechtmäßig war?

Die Fragen 10 bis 10c werden zusammen beantwortet.

Eine Auswertung der Protokolldaten erfolgt bislang anlassbezogen und mit Anordnung der Behördenleitung.

Der im Zollfahndungsdienst bestehende Geschäftsprozess zur Auswertung von Protokolldateien zu den gesetzlich vorgegebenen Zwecken wurde kürzlich weiter formalisiert. In einem nächsten Schritt werden mit der Überarbeitung des Datenschutzkonzeptes für den Zollfahndungsdienst regelmäßige, stichprobenhafte Kontrollen verbindlich festgelegt.

11. Wie häufig kam es 2017, 2018, 2019 und im ersten Halbjahr 2020 zu unrechtmäßigen Datenabfragen durch die Zollverwaltung bzw. Mitarbeiterinnen und Mitarbeiter der Zollverwaltung?

In dem o. g. Zeitraum wurde ein Fall in 2018 und zwei Fälle in 2019 von möglichen unrechtmäßigen Abfragen der polizeilichen Verbunddaten bekannt. Der Verdacht der Unrechtmäßigkeit hat sich in dem einen Fall aus 2018 und einem Fall aus 2019 bestätigt. In dem zweiten Fall aus 2019 ergab die Überprüfung, dass die Abfrage rechtmäßig erfolgte.

a) Welche Art von Daten sowie welche Datenbanken waren davon betroffen (bitte so vollständig wie möglich angeben)?

Die Abfragen bezogen sich auf personenbezogene Daten aus den Systemen INZOLL und INPOL-Zoll.

b) Inwiefern konnte festgestellt werden, ob die unrechtmäßig abgefragten Daten innerhalb der Behörde oder an externe Personen weitergeleitet wurden, und falls letzteres zutrifft, welche Angaben kann die Bundesregierung zu diesen Personen machen?

Eine Weitergabe von Daten innerhalb der Behörde oder an externe Personen hat nicht stattgefunden.

c) Inwiefern konnten die hierfür verantwortlichen Mitarbeiterinnen und Mitarbeiter namentlich zugeordnet werden?

Die verantwortlichen Personen konnten anhand der individuellen Benutzerkennung ermittelt werden.

d) Welche Motive für die unrechtmäßigen Datenabfragen konnten ermittelt werden?

Es wurden persönliche Gründe und die Sorge um die eigene Familie angegeben.

e) Welche disziplinarischen oder rechtlichen Konsequenzen wurden gezogen?

Es wurde ein behördliches Disziplinarverfahren mit Verhängung einer Disziplinarmaßnahme durchgeführt. In einem Fall wurde das Beschäftigungsverhältnis beendet.

f) Welche weiteren Schlussfolgerungen wurden aus den Vorfällen gezogen?

Es erfolgen zusätzliche, fallbezogene Sensibilisierungen der Mitarbeiter und Mitarbeiterinnen über die regelmäßigen Bekanntmachungen hinaus.

12. An welchen gemeinsamen Datenbanken mit ausländischen Sicherheitsbehörden beteiligen sich die polizeilichen Sicherheitsbehörden des Bundes?

Das BKA beteiligt sich an dem Schengener Informationssystem (SIS), in das es selbst Datensätze einstellen bzw. Fahndungen ausländischer Sicherheitsbehörden abrufen kann. Das BKA kann auf Datensätze des EIS (Europol Information System) und des CtW (Check the Web, ein auf Webtechnologie basierendes Portal mit dahinterliegender Datenbank zur Recherche nach Webseiten und Verlautbarungen von Organisationen und Personen aus dem Phänomenbereich des islamistischen Terrorismus, vgl. Bundestagsdrucksache 18/4035) von EUROPOL zugreifen, zudem auf folgende Interpol-Dateien:

DIAL DOC, DNA, EDISON, Facial Recognition, Fingerprints, Foreign Terrorist Fighters, ICIS (Nominal), ICSE, Maritime Security, Millennium, Stolen Administrative Documents, SLTD (Stolen and Lost Travel Documents), Stolen Motor Vehicles, Stolen Vessels Database, Works of Art.

Die Bundespolizei beteiligt sich an folgenden gemeinsamen Informationssystemen:

- SIS,
- Interpol (SLTD) und
- EIS.

Der Zollfahndungsdienst arbeitet mit den ausländischen Sicherheitsbehörden Europol und Interpol zusammen. Ein Datenaustausch erfolgt mit dem Europol-Informationssystem. Allerdings werden gemäß entsprechender Relevanzkriterien lediglich Daten ans Informationssystem übermittelt. Abfragen können über die zugehörige Schnittstelle nicht gestellt werden. Insofern entfällt auch die Beantwortung der Unterfragen zu 12a und 12b.

a) Welche Sicherungsmaßnahmen gegen unrechtmäßige Datenabfragen gibt es dabei (bitte ggf. unterscheiden, falls die Sicherungsmaßnahmen für die deutschen Sicherheitsbehörden von denen ausländischer Sicherheitsbehörden abweichen)?

Beim BKA gelten hinsichtlich des Zugriffs auf gespeicherte Dateien in den (gemeinsamen) Datenbanken mit ausländischen Sicherheitsbehörden auch hier die Regelungen zu den Zugriffsberechtigungen. Bei EUROPOL und Interpol werden die Zugriffe protokolliert und die Systeme auf einem dem BKA vergleichbaren Standard des technischen Datenschutzes und der IT-Sicherheit geschützt.

Bei der Bundespolizei gilt für die Nutzung der Informationssysteme das Rollen- und Rechtekonzept inklusive der daraus resultierenden Schutzmaßnahmen. Bezüglich weiterer technischer Details wird auf die Beantwortung zu Frage 6 verwiesen.

b) Wie häufig kam es 2017, 2018, 2019 und im ersten Halbjahr 2020 zu unrechtmäßigen Datenabfragen aus diesen Dateien durch Sicherheitsbehörden des Bundes bzw. durch Mitarbeiterinnen und Mitarbeiter dieser Sicherheitsbehörden bzw. nach Kenntnis der Bundesregierung durch ausländische Sicherheitsbehörden oder deren Mitarbeiterinnen und Mitarbeiter, und welche weiteren Angaben kann die Bundesregierung diesbezüglich zu Verantwortlichen, Datenbanken, Art der Daten, mögliche Weitergabe, politische Hintergründe und Konsequenzen machen?

Es liegen keine Erkenntnisse dazu vor, dass es durch Mitarbeiterinnen und Mitarbeiter zu unrechtmäßigen Abfragen in (gemeinsamen) Datenbanken mit ausländischen Sicherheitsbehörden kam.

13. Hält die Bundesregierung eine besondere Sicherung der Staatsschutzdateien gegen unrechtmäßige Datenabfrage für erforderlich, und wenn ja, inwiefern, und was will sie diesbezüglich ggf. unternehmen?

Über die bestehenden Berechtigungskonzepte ist der Zugriff auf Staatsschutzdateien auf einen engen Personenkreis beschränkt, der unmittelbar mit Aufgaben betraut ist, zu deren Erfüllung die Nutzung der Dateien erforderlich ist. Die geringe Anzahl von festgestelltem Missbrauch deutet darauf hin, dass die bestehenden Maßnahmen, z. B. Überprüfungen der Beschäftigten nach dem Sicherheitsüberprüfungsgesetz, die vollständige Protokollierung und die Stichprobenkontrollen wirksam sind. Es ist daher keine weitergehende „besondere Sicherung“ erforderlich.

14. Hält die Bundesregierung eine signifikante Reduzierung des Datenbestandes in den Polizeidatenbanken insbesondere bei den Staatsschutzdateien für geboten, um das Risiko für die Personen, über die darin Daten gespeichert werden, zu reduzieren, und wenn ja, inwiefern?

Der Datenbestand ergibt sich aus den gesetzlichen Bestimmungen und den fachlichen Erfordernissen einer effektiven Gefahrenabwehr und Strafverfolgung.

15. Welche Sicherungsmechanismen gegen unrechtmäßige Datenabfragen gibt es im Bereich der Geheimdienste und des nachrichtendienstlichen Informationsverbundes (bitte so umfassend wie möglich darstellen)?

Für alle IT-Systeme des Bundesamtes für Verfassungsschutz (BfV) werden vor Inbetriebnahme IT-Sicherheitskonzepte erstellt. Darin werden u. a. Maßnahmen zur Verhinderung unberechtigter Zugriffe festgelegt. Hierbei handelt es sich um Berechtigungskonzepte, zusätzlich wird eine vollinhaltliche Protokollierung (revisionssicher) durchgeführt. Die Systeme werden gemäß den Grundschutzrichtlinien des BSI gehärtet und es erfolgt eine regelmäßige Sensibilisierung der Benutzerinnen und Benutzer. Es wird davon ausgegangen, dass mit dem „nachrichtendienstlichen Informationsverbund“ das Nachrichtendienstliche Informationssystem (NADIS) als zentrales fachliches Verbundsystem der Verfassungsschutzbehörden des Bundes und der Länder, das diese bei der Aufgabenerfüllung nach § 3 des Verfassungsschutzgesetzes (BVerfSchG) und der Erfüllung der gegenseitigen Unterrichtungspflichten nach § 6 Absatz 1 BVerfSchG unterstützt, gemeint ist. Der Zugriff auf das NADIS ist auf jene Mitarbeiterinnen und Mitarbeiter der Verfassungsschutzbehörden und – im Rahmen des § 3 Absatz 3 Satz 4 des MAD-Gesetzes (MADG) – des Militärischen Abschirmdienstes (MAD) beschränkt, die unmittelbar mit Aufgaben betraut sind, zu deren Erfüllung die Nutzung des NADIS erforderlich ist (umfangreiches Rollen- und Berechtigungskonzept). Darüber hinaus sind beim Systemzugriff Maßnahmen der Zugangs-, Speicher- und Zugriffskontrolle gemäß § 64 Absatz 3 Satz 1 Nummer 1, 3 und 5 BDSG i. V. m. § 6 Absatz 3 Satz 1 BVerfSchG entsprechend dem heutigen Stand der Technik gewährleistet.

Weiterhin wird gemäß § 6 Absatz 3 Satz 2 BVerfSchG für Zwecke der Datenschutzkontrolle bei jedem Zugriff der Zeitpunkt, die Angaben, die die Feststellung der abgefragten Datensätze ermöglichen, sowie die abfragende Stelle protokolliert. Die Zweckbindung für Zwecke der Datenschutzkontrolle schließt auch die Feststellung unberechtigter Kenntnisnahme von Daten sowie Folgemaßnahmen ein, die an Verstöße anknüpfen, insbesondere eine disziplinar- oder strafrechtliche Sanktionierung.

Der MAD verfügt über ein eigenes Datenschutzkonzept, das den Mitarbeiterinnen und Mitarbeitern Handlungssicherheit im Umgang mit Daten gibt und zu einer Erhöhung des Datenschutzbewusstseins beiträgt. Alle Mitarbeiterinnen und Mitarbeiter des MAD sind sicherheitsüberprüft und erfüllen somit die formalen Voraussetzungen als Geheimnisträger für den verantwortungsbewussten, rechtmäßigen Umgang mit sensiblen Daten. Überdies finden regelmäßig Sensibilisierungen der Mitarbeiterinnen und Mitarbeiter des MAD zum rechtmäßigen Umgang mit Daten statt.

Systemseitig werden bei den Fachdateien und IT-Systemen Protokolldaten erzeugt. Diese können im Rahmen von Kontrollen ausgelesen werden und lassen folglich Rückschlüsse auf die Verarbeitung der jeweiligen Daten zu. Des Weiteren werden die Mitarbeiterinnen und Mitarbeiter im Rahmen eines festgelegten Rechte-/Rollenkonzeptes ausschließlich für die zur jeweiligen Aufgabenerfüllung notwendigen Daten freigeschaltet.

Zur Kontrolle von Datenabfragen erfolgen regelmäßig sogenannte Datenschutzaudits. Zu diesem Zweck wurde ein eigenes Prüf-/Auditingkonzept erstellt. In diesem werden regelmäßige und anlassbezogene Prüfungen erstellt.

Zum BND wird auf die Vorbemerkung der Bundesregierung und die Anlage mit der Einstufung „VS – Nur für den Dienstgebrauch“ verwiesen.[1]

16. Wie häufig kam es 2017, 2018, 2019 und im ersten Halbjahr 2020 zu unrechtmäßigen Datenabfragen durch das Bundesamt für Verfassungsschutz (BfV), den Bundesnachrichtendienst (BND), den Militärischen Abschirmdienst (MAD) oder einen anderen (ausländischen) Nachrichtendienst oder jeweils dessen Mitarbeiterinnen und Mitarbeiter?

Für den BND kann die Antwort auf die Frage nicht offen erfolgen. Die Einstufung der Antwort auf die Fragen als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Vertraulich“ ist im vorliegenden Fall im Hinblick auf Gründe des Staatswohls erforderlich.[2]

Nach der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern, für Bau und Heimat zum materiellen und organisatorischen Schutz von Verschlusssachen (Verschlusssachenanweisung – VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein können, entsprechend einzustufen. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Fragen würde Informationen zu den Fähigkeiten und Methoden des Bundesnachrichtendienstes einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen.

Eine Beantwortung der angefragten Informationen kann nur als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Vertraulich“ erfolgen und wird dem Deutschen Bundestag gesondert übermittelt.[2]

Einzelheiten zu den Fragen 16 bis 16f können für das BfV und den MAD aus Gründen des Staatswohls nicht öffentlich dargestellt werden, da sich aus ihrer Beantwortung Einblicke in die methodische Vorgehensweise des BfV und des MAD bei Ermittlungen im Zusammenhang mit dienstinternen Verstößen ergeben. Darüber hinaus sind die Angaben geeignet, Anhaltspunkte zu bieten, welche eine Bewertung des möglichen Einflusses entsprechender Umstände auf die Integrität der Mitarbeiter und damit auf die Leistungsfähigkeit des BfV und des MAD zulassen.

Die Kenntnisnahme durch Unbefugte kann für die Interessen der Bundesrepublik Deutschland nachteilig sein. Deshalb sind die Informationen als „VS – Nur für den Dienstgebrauch“ eingestuft (vgl. Anlage VS – NfD).[1]

a) Welche Art von Daten sowie welche Datenbanken waren davon betroffen (bitte so vollständig wie möglich angeben)?

b) Inwiefern konnte festgestellt werden, ob die unrechtmäßig abgefragten Daten innerhalb der Behörde oder an externe Personen weitergeleitet wurden, und falls letzteres zutrifft, welche Angaben kann die Bundesregierung zu diesen Personen machen?

c) Inwiefern konnten die hierfür verantwortlichen Mitarbeiterinnen und Mitarbeiter namentlich zugeordnet werden?

---

[1] Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

[2] Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Vertraulich“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

d) Welche Motive für die unrechtmäßigen Datenabfragen konnten ermittelt werden?

e) Welche disziplinarischen oder rechtlichen Konsequenzen wurden durchgeführt?

f) Welche weiteren Schlussfolgerungen wurden aus den Vorfällen gezogen?

Für den Bereich des BND wird auf die Antwort zu Frage 16 und die Anlage mit der Einstufung „VS – Vertraulich“ verwiesen.[3]

Für den Bereich des BfV und MAD wird auf die Antwort zu Frage 16 und die Anlage mit der Einstufung „VS – Nur für den Dienstgebrauch“ verwiesen.[4]

17. Welche Sicherungsmechanismen gegen unrechtmäßige Datenabfragen bei gemeinsam von BfV bzw. BND mit ausländischen Nachrichtendiensten geführten Dateien gibt es, und wie häufig konnten 2017, 2018, 2019 und 2020 unrechtmäßige Datenabfragen festgestellt werden (bitte soweit möglich nach dem Schema der Frage 16 beantworten)?

Gegenstand der Frage sind solche Informationen, die in besonders hohem Maße das Staatswohl berühren. Die Bundesregierung ist nach sorgfältiger Abwägung der in diesem Fall widerstreitenden Interessen zu der Auffassung gelangt, dass die Frage selbst in eingestufter Form nicht beantwortet werden kann. Das verfassungsrechtlich verbürgte Frage- und Informationsrecht des Deutschen Bundestages gegenüber der Bundesregierung wird durch gleichfalls Verfassungsrang genießende schutzwürdige Interessen wie das Staatswohl begrenzt. Eine Offenlegung der angefragten Informationen birgt die Gefahr, dass Einzelheiten insbesondere zur Arbeitsweise und zu dem damit einhergehenden Informationsaustausch bekannt würden, die unter dem Aspekt des Schutzes der nachrichtendienstlichen Zusammenarbeit mit ausländischen Partnern besonders schutzbedürftig sind. Eine öffentliche Bekanntgabe von Informationen zur technischen Leistungsfähigkeit sowie zur Methodik von ausländischen Nachrichtendiensten und damit einhergehend die Kenntnisnahme durch Unbefugte würde erhebliche nachteilige Auswirkungen auf die vertrauensvolle Zusammenarbeit mit diesen haben. Würden in der Konsequenz eines Vertrauensverlustes Informationen von ausländischen Stellen entfallen oder wesentlich zurückgehen, entstünden signifikante Informationslücken mit negativen Folgewirkungen für die Genauigkeit der Abbildung betreffend Informationen zur Sicherheitslage in der Bundesrepublik Deutschland sowie im Hinblick auf den Schutz deutscher Interessen im Ausland.

Dies würde folgenschwere Einschränkungen der Informationsgewinnung zur Folge haben, womit letztlich der gesetzliche Auftrag des Bundesnachrichtendienstes – die Sammlung und Auswertung von Informationen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind (§ 1 Absatz 2 BNDG) – nicht mehr sachgerecht erfüllt werden könnte. Die Gewinnung von auslandsbezogenen Informationen ist für die Sicherheit der Bundesrepublik Deutschland und für die Aufgabenerfüllung des Bundesnachrichtendienstes jedoch unerlässlich. Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die

[3] Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Vertraulich“ eingestuft. Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

[4] Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Bedeutung für die Aufgabenerfüllung des Bundesnachrichtendienstes nicht ausreichend Rechnung tragen. Die angefragten Inhalte beschreiben die Fähigkeiten und Arbeitsweisen des Bundesnachrichtendienstes so detailliert, dass eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern ihrem Schutzbedürfnis nicht Rechnung tragen kann. Bei einem Bekanntwerden der schutzbedürftigen Information wäre kein Ersatz durch andere Instrumente der Informationsgewinnung möglich. Aus dem Vorgesagten ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht wesentlich überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber dem Geheimhaltungsinteresse der Bundesregierung zurückstehen. Dabei ist der Umstand, dass die Antwort verweigert wird, weder als Bestätigung noch als Verneinung des angefragten Sachverhaltes zu werten.

18. Inwiefern gelten für Datenabfragen der Staatsanwaltschaften im INPOL-System sowie der Polizeibehörden aus dem Datenbestand der Staatsanwaltschaften (Zentrales Staatsanwaltschaftliches Verfahrensregister) vergleichbare Kontroll- bzw. Abschreckungsmechanismen (bitte möglichst detailliert ausführen)?

Staatsanwaltschaften dürfen Auskünfte grundsätzlich nur einholen, wenn dies in einem konkreten Verfahren erforderlich ist (§ 161 Absatz 1 der Strafprozessordnung – StPO).

Die Abfrage setzt jedenfalls voraus, dass die Staatsanwaltschaft die Einleitung eines Ermittlungsverfahrens prüft oder ein Ermittlungs-, Straf- oder Vollstreckungsverfahren anhängig ist. Zudem ist eine registermäßige Erfassung erforderlich.

Abfragen der Staatsanwaltschaften sind nur möglich, wenn hierfür ein elektronischer Zugang zwischen der Staatsanwaltschaft und dem Zentralen Staatsanwaltlichen Verfahrensregister (ZStV) eingerichtet ist. Wie die Staatsanwaltschaften die Zugangsberechtigungen auf ihre Dateisysteme ausgestalten, richtet sich nach dem jeweiligen Rechte-Rollen-Management der jeweiligen Behörden. Hierüber liegen der Bundesregierung keine Kenntnisse vor.

Beim Generalbundesanwalt beim Bundesgerichtshof kann eine Abfrage durch einen eingeschränkten Personenkreis erfolgen, der mit der Bearbeitung der Auskünfte betraut ist.

Ein Zugriff der Staatsanwaltschaften auf das INPOL-System ist derzeit noch nicht möglich.

Die Bundespolizei und das BKA haben keinen Zugriff auf das zentrale Staatsanwaltschaftliche Verfahrensregister.

19. Wie häufig kam es nach Kenntnis der Bundesregierung in den Jahren 2017, 2018, 2019 und im ersten Halbjahr 2020 zu unrechtmäßigen Abfragen von Sicherheitsbehörden des Bundes in Dateien der Staatsanwaltschaften und umgekehrt (bitte soweit möglich nach dem Schema der Frage 8 beantworten)?

Bei den Dateien der Staatsanwaltschaften handelt sich um Dateien der Länder, über die die Bundesregierung keine Erkenntnisse hat.

Für den angefragten Zeitraum sind auch keine unrechtmäßigen Abfragen des Zentralen Staatsanwaltschaftlichen Verfahrensregisters durch die Zollverwaltung bekannt.

20. Auf welche anderen Dateien haben Sicherheitsbehörden des Bundes Zugriff, welche Sicherungsmechanismen gegen unrechtmäßige Datenabgriffe gibt es, und wie häufig konnten 2017, 2018, 2019 und im ersten Halbjahr 2020 unrechtmäßige Datenabfragen festgestellt werden (bitte für jedes Dateisystem getrennt und soweit möglich nach dem Schema der Frage 8 beantworten)?

Im BKA können Beschäftige des BKA (entsprechend ihrer Berechtigung) auf folgende, nicht-polizeiliche Dateien zugreifen:

- Automatisierte Liegenschaftsbücher (Hessen und Berlin)
- Ausländerzentralregister,
- VISA-Informationssystem (VIS),
- EURODAC (Europäisches System für den Abgleich der Fingerabdruckdaten von Asylbewerbern),
- Bundeszentralregister,
- Gewerberegister Berlin und Schleswig-Holstein,
- Einwohnermeldedaten der einzelnen Bundesländer,
- Grundbuchportale der einzelnen Bundesländer,
- Datenbank Bundesnetzagentur,
- Nationales Waffenregister,
- ZEVIS,
- EUCARIS (europäische Fahrzeug- und Fahrerlaubnisregisterdaten) und
- Handels-, Vereins-, Partnerschafts- und Genossenschaftsregister NRW.

Dabei kommen die für die jeweiligen Dateien zugrundeliegenden Sicherheitsmechanismen zum Tragen und können bei den Datei-führenden Stellen erfragt werden. Die Zugriffe für BKA-Beschäftige ergeben sich aus den o. g. Benutzerkonzepten.

Für die Bundespolizei wird auf die Antwort zu den Fragen 1 und 8 verwiesen. Darüber hinaus besteht Zugriff auf folgende Dateien:

- Nationales Waffenregister,
- EURODAC,
- VISA-Informationssystem und
- Datenbank Bundesnetzagentur.

Das BfV darf auf Grundlage gesetzlicher Befugnisse auf folgende Dateien im automatisierten Abrufverfahren zugreifen:

- Zentrales Fahrzeugregister beim Kraftfahrt-Bundesamt,
- Melderegister,
- Personalausweisregister (bezogen auf den Abruf des Lichtbildes),
- Passregister (bezogen auf den Abruf des Lichtbildes),
- Nationales Waffenregister,
- Ausländerzentralregister,
- VISA-Informationssystem,
- die beim Auswärtigen Amt geführte Datei FREMIS (Fremde Mission).

Des Weiteren darf das BfV im Rahmen eines automatisierten Verfahrens Auskunftsanfragen an

- das Bundeszentralregister,
- das Zentrale Staatsanwaltschaftliche Verfahrensregister und
- die Bundesnetzagentur

richten.

Der Zugriff auf die vorgenannten Dateien ist auf Mitarbeiterinnen und Mitarbeiter der Verfassungsschutzbehörden beschränkt, die hierzu besonders ermächtigt sind. Die Zugriffe im automatisierten Abrufverfahren werden darüber hinaus systemseitig protokolliert, wobei in Bezug auf die Zugriffe des BfV auf das Nationale Waffenregister, Melderegister, das Personal- und Passregister (bezogen auf den Abruf des Lichtbildes) und das Ausländerzentralregister kraft gesetzlicher Bestimmungen die Protokollierung der Zugriffe beim BfV selbst zu erfolgen hat. Darüber hinaus ist gemäß § 492 Absatz 4 Satz 2 StPO i. V. m. § 18 Absatz 5 Satz 2 BVerfSchG bei ZStV-Anfragen für Kontrollzwecke ein entsprechender Nachweis beim BfV zu führen, aus dem der Zweck und die Veranlassung, die ersuchte Behörde und die Aktenfundstelle hervorgehen. Diese Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr ihrer Erstellung folgt, zu vernichten. Im Zuge jährlicher Belehrungen werden die Mitarbeiterinnen und Mitarbeiter des BfV über die Strafbarkeit bzw. arbeits-/dienstrechtlichen Konsequenzen unrechtmäßiger Dateiabfragen belehrt. Ferner werden die Mitarbeiterinnen und Mitarbeiter bei besonderen Vorkommnissen (z. B. nach Bekanntwerden der Vorkommnisse in Hessen – NSU 2.0) gesondert sensibilisiert.

In einem Fall wurden Datensätze (von Familien- und BfV-Angehörigen) beim Einwohnermeldeamt abgefragt. Eine Weiterleitung der Daten konnte im Rahmen der Aufklärung des Falles nicht festgestellt werden. Die zwei verantwortlichen Personen konnten identifiziert werden. Das Handeln war durch Neugier motiviert. Es erfolgten arbeitsrechtliche Maßnahmen. Im diesem Fall erwiesen sich die Verwaltungsermittlungen als geeignet, die entsprechenden Verstöße aufzuklären.

Ende 2019 fand aufgrund einer Verwechslung mit der namensähnlichen VISA-Datei des Bundesverwaltungsamtes (Teil des AZR), auf die eigentlich ein autorisierter Zugriff erfolgen sollte, ein unbegründeter und damit unzulässiger Datenabruf im VIS statt, der allerdings keinen Treffer ergab. Die verantwortliche Person im BfV konnte identifiziert werden; es handelte sich um ein Versehen. Die Person wurde nochmals belehrt, arbeitsrechtliche Folgen ergaben sich nicht. Die internen Kontrollmechanismen waren auch in diesem Fall geeignet, den Vorfall aufzuklären.

Die Zollverwaltung darf auf Grundlage gesetzlicher Bestimmungen auf die folgenden nicht-polizeilichen/zolleigenen Register oder Datenbanken zugreifen:

- Ausländerzentralregister,
- Bundeszentralregister,
- Einwohnermeldedaten der einzelnen Bundesländer,
- Grundbuch–Online,
- Gewerbezentralregister,
- Handelsregister,
- Kontoabrufverfahren,
- Nationales Waffenregister,

- Orbis (Unternehmensberichte),
- SteuerID-Datenbank,
- Transparenzregister,
- Umsatzsteuer Länder Online
- VISA-Informationssystem,
- Zentrales Fahrzeugregister,
- Zentrales Staatsanwaltschaftliches Verfahrensregister und
- Zentrales Verkehrsinformationssystem.

Bei Zugriffen auf die verschiedensten Datensysteme werden die jeweils geltenden Datenschutz- und Sicherungsmaßnahmen beachtet. Zu den Kontrollmechanismen zählen insbesondere Rollen- und Rechtekonzepte, die Protokollierung sowie anlassbezogene und stichprobenweise Prüfungen.

Im o. g. Zeitraum wurden zwei Fälle in 2017, ein Fall in 2018 und zwei Fälle in 2019 von unrechtmäßigen Abfragen in Datensystemen bekannt. In allen Fällen handelte es sich um Abfragen der Einwohnermeldedaten. Die Abfragen bezogen sich auf Einwohnermeldedaten zu Personen aus dem kollegialen bzw. privaten Umfeld.

Eine Weitergabe von Daten innerhalb der Behörde oder an externe Personen hat nicht stattgefunden.

Die verantwortlichen Personen konnten anhand individueller Benutzerkennungen ermittelt werden. Es wurden persönliche bzw. private Motive angegeben, wie z. B. eine familiäre Auseinandersetzung, sowie die vorgebliche Überprüfung der Funktionsfähigkeit des Systems. Es kam zur Ahndung durch Geldbuße bzw. Verweis im Rahmen eines Disziplinarverfahrens. Es erfolgen zusätzliche, fallbezogene Sensibilisierungen der Mitarbeiter und Mitarbeiterinnen über die regelmäßigen Bekanntmachungen hinaus.

Für den BND wird auf die Vorbemerkung der Bundesregierung und die Anlage mit der Einstufung „VS – Nur für den Dienstgebrauch“ verwiesen.[5]

Zur Aufgabenerfüllung fragt der MAD andere Behörden des Bundes um Übermittlung erforderlicher Informationen an. Diese Abfragen werden protokolliert und erfahren eine jährliche Prüfung auf Rechtmäßigkeit der Abrufe bzw. der Nutzung.

Einzige Schnittstelle ist der lesende Zugriff auf der Plattform „Nachrichtendienstliches Informationssystems (NADIS)“. Hier ist der MAD berechtigt, Abfragen direkt in NADIS zu stellen.

Die Rechtmäßigkeit der Datenabfragen ist über die Auswertung der Protokolldaten (auf welche Daten wurde durch wen, wann und in welchem Umfang zugegriffen?) ermittelbar.

Für den angegebenen Zeitraum sind keine unrechtmäßigen Abfragen bekannt.

[5] Das Bundesministerium des Innern, für Bau und Heimat hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333