**Deutscher Bundestag** **Drucksache 19/2374**

**19. Wahlperiode** 30.05.2018

# Antwort

## der Bundesregierung

**auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Heike Hänsel, Ulla Jelpke, weiterer Abgeordneter und der Fraktion DIE LINKE.**
**– Drucksache 19/2077 –**

## Datenaustausch im Rahmen der geheimdienstlichen europäischen „Gruppe für Terrorismusbekämpfung“ (CTG)

Vorbemerkung der Fragesteller

Nach einer Gesetzesänderung vom Sommer 2016 kooperiert das Bundesamt für Verfassungsschutz (BfV) mit 29 europäischen Geheimdiensten in Den Haag. In einer „operativen Plattform“ wird dort beim niederländischen Inlandsgeheimdienst AIVD eine gemeinsame Datenbank geführt. Diese gehört zu der im Jahr 2001 gegründeten „Counter Terrorism Group“ (CTG) des sog. „Berner Clubs“, dem informellen Zusammenschluss von Inlandsgeheimdiensten der EU-Mitgliedstaaten sowie Norwegens und der Schweiz. Wiederholt hat sich die Fraktion DIE LINKE. nach der Auslandstätigkeit des BfV in Den Haag erkundigt, etwa auf Bundestagsdrucksachen 18/11361, 18/10457, 18/8016, 18/9222, 18/9836, 18/7773, 18/4917. In keinem Fall hat die Bundesregierung wesentliche Informationen mitgeteilt oder wenigstens als Verschlusssache in der Geheimschutzstelle hinterlegt. Weder nennt das Bundesministerium des Innern, für Bau und Heimat teilnehmende Dienste noch erfahren die Fragesteller Einzelheiten zu Arbeitsgruppen, Personal und Kosten des Zentrums. Auch der konkrete Ort, die Beschaffenheit der CTG-Datenbank, dort geführte Datenfelder oder eingesetzte Such- und Analysewerkzeuge bleiben geheim.

Jetzt hat die niederländische Kommission für die Überwachung der Nachrichten- und Sicherheitsdienste (CTIVD) die „operative Plattform“ kontrolliert (http://gleft.de/2cf). Unter der gesetzlichen Schweigepflicht erhielt der Ausschuss dafür Einsicht in alle gewünschten Daten und kam unter anderem zu dem Ergebnis, dass in einigen Fällen die Bereitstellung von Informationen durch den AIVD „sorglos“ gewesen sei. Erstmals erfährt die Öffentlichkeit Details zum Datentausch: Wenn eine der beteiligten Stellen Daten einspeist, werden diese an alle anderen beteiligten Behörden weitergeleitet. Möglich ist auch die „multilaterale“ Teilung von Informationen unter vorher definierten Partnern. Der Fokus liegt laut der CTIVD auf „(angeblichen) Dschihadisten“. Dem AIVD obliegt eine federführende Rolle bei der Errichtung und Führung der „operativen Plattform“ bzw. der angeschlossenen Datenbank, die offiziell erst im Januar 2017 in Betrieb genommen wurde und auf einem Server in den Niederlanden liegt. Die Datenbank sei laut dem CTIVD „im Herbst 2017 durch den AIVD

*Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 24. Mai 2018 übermittelt.*

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

umgebaut“ worden. Im August 2017 hatte der AIVD interne Regularien festgelegt, wonach nur Daten, von deren Richtigkeit ausgegangen werden kann, an die Datenbank weitergegeben werden können.

Da es sich in der Datenbank nicht nur um strategische oder operative Informationen handelt, sondern personenbezogene Daten ausgetauscht werden, sind hierfür auch entsprechende niederländische Kontrollkommissionen zuständig. Laut der CTIVD seien dafür die allgemeinen niederländischen Datenschutzgrundsätze maßgeblich. Der AIVD agiere als „faktischer Geschäftsführer“ der Datenbank, ihm oblägen daher Sorgfaltsplichten wie die Verpflichtung zur Gewährleistung des Schutzes personenbezogener Daten und zur Verhinderung von Sicherheitsverletzungen. Die Konzeption der „operativen Plattform“ müsse daher ausreichend Garantien und deren Überprüfung sicherstellen.

Für die Gewährleistung eines „angemessenen Datenschutzniveaus“ seien der CTIVD zufolge „grundsätzlich“ auch die anderen 29 Partner verantwortlich. Die gemeinsame Verantwortung sei bei einer Verletzung des Datenschutzes als „gesamtschuldnerische Haftung“ auszulegen. Hierzu müssten „klare Vereinbarungen über den Datenaustausch und die Anwendung gemeinsamer Normen für jede Vertragspartei“ beschlossen werden, was laut der CTIVD bislang nur in begrenztem Umfang umgesetzt worden sei. Erforderlich seien deshalb Vereinbarungen über den Austausch, die Speicherung und die Verarbeitung der Daten sowie die Befugnisse und Pflichten jeder beteiligten Partei. Das Maß an Datenschutz müsse mindestens der Europäischen Menschenrechtskonvention (EMRK) entsprechen. Es müsse beispielsweise für die Nutzerinnen und Nutzer hinreichend klar sein, auf der Grundlage und nach welchen Kriterien eine Person in die Datenbank aufgenommen wird.

Zu den Empfehlungen der CTIVD gehören eine Definition der Ziele der Datenbank und ihre Begrenzungen hinsichtlich einer Speicherung. Unrichtige oder nicht mehr relevante Daten müssten gelöscht werden. Zudem müssten Kriterien für den Austausch von Daten über Minderjährige definiert werden. Auch die Zugangsberechtigungen zu der Datenbank und die Vergabe von Schreibrechten seien nicht ausreichend eingeschränkt.

Außerdem empfiehlt die Kommission die engere Zusammenarbeit nationaler Aufsichtsbehörden bzw. Kontrollorgane, denen bestimmte Aufgaben zugewiesen werden könnten. In nur einem Projekt arbeiteten diesbezüglich fünf zuständige Gremien zusammen, die sich jedoch wegen der gesetzlichen Schweigepflicht nicht untereinander über Angelegenheiten austauschen dürfen, die als Staatsgeheimnisse klassifiziert sind. Diese Einschränkungen müssten der CTIVD zufolge aufgehoben werden. Eine andere Option sei die explizite Zuweisung einzelner Kontrollaufgaben an eine oder mehrere Aufsichtsbehörden. Schließlich sei auch eine übergeordnete, internationale Aufsicht denkbar. Eine solche Stelle müsse jedoch erst eingerichtet werden und erfordere entsprechende vertragliche Vereinbarungen der 30 teilnehmenden Geheimdienste.

## Vorbemerkung der Bundesregierung

Die Bundesregierung geht auch in dieser Kleinen Anfrage davon aus, dass mit „Geheimdiensten“ und „Inlandsgeheimdiensten der EU-Mitgliedstaaten“ die Nachrichtendienste gemeint sind.

Die Beantwortung der Fragen 4, 5, 5a, 5b, 6, 8c, 9 und 10 kann im Hinblick auf das Staatswohl nicht offen erfolgen. Nach § 3 Nummer 4 der Allgemeinen Verwaltungsvorschrift 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 Kooperationen mit einer Vielzahl von ausländischen Nachrichtendiensten einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Die Vertraulichkeit der Zusammenarbeit von Nachrichtendiensten ist wesentliche Grundlage für eine vertrauensvolle Kooperation. Neben der Zusammenarbeit als solcher würden durch die Veröffentlichung auch Informationen zu Fähigkeiten und Aufklärungsschwerpunkten anderer Nachrichtendienste und indirekt auch außenpolitische Zielsetzungen und Interessen anderer Staaten offenbart. Eine Öffentlichmachung der Zusammenarbeit anderer Nachrichtendienste mit Nachrichtendiensten des Bundes entgegen der (mindestens stillschweigend) zugesicherten Vertraulichkeit würde nicht nur die Nachrichtendienste des Bundes in grober Weise diskreditieren, es könnten sich zudem Nachteile für die zukünftige Zusammenarbeit mit ausländischen Nachrichtendiensten ergeben. Der Rückgang des Informationsaustausches mit anderen Nachrichtendiensten könnte eine Verschlechterung der Einschätzung der Sicherheitslage durch die deutschen Nachrichtendienste zur Folge haben.

Im Ergebnis kann die Veröffentlichung der angefragten Informationen für die wirksame Erfüllung der gesetzlichen Aufgaben der deutschen Nachrichtendienste und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein. Diese Informationen werden daher gemäß § 3 Nummer 4 VSA als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.*

1. Inwiefern hat sich die Bundesregierung zur Beantwortung der Kleinen Anfragen auf Bundestagsdrucksachen 19/489, 18/11577, 18/10641, 18/8170, 18/9323, 18/9974, 18/7930, 18/5048 jemals bei der „Counter Terrorism Group“ (CTG) um Freigabe der von den Abgeordneten erbetenen und schließlich geheim gehaltenen Informationen bemüht?

Es wird bei der Beantwortung parlamentarischer Anfragen stets geprüft, ob diesbezügliche Freigabeanfragen bei den betroffenen CTG-Diensten in Frage kommen. Liegt eine Freigabe nicht vor, nimmt die Bundesregierung eine Abwägung vor, bei der das parlamentarische Informationsinteresse gegen das Interesse an der Erhaltung der außen- und sicherheitspolitischen Handlungsfähigkeit der Bundesregierung abgewogen wird. Zu berücksichtigen ist dabei, dass eine Weitergabe ohne Einverständnis der übermittelnden Stelle dem den nachrichtendienstlichen Verkehr prägenden Informationsbeherrschungsrecht widerspricht. Ein Verstoß gegen diese Grundsätze kann zur Folge haben, dass der Empfängerstaat von der übermittelnden Stelle keine weiteren Informationen mehr erhält. Darüber hinaus könnte ein Verstoß zur Folge haben, dass der ausländische Dienst auch seinerseits die Vertraulichkeit übermittelter deutscher Informationen nicht oder nur noch eingeschränkt wahren würde. Es ist dann zu befürchten, dass das Bundesamt für Verfassungsschutz (BfV) nicht mehr in der Lage ist, die ihm gesetzlich übertragenen Aufgaben zu erfüllen.

* Das Bundesministerium des Innern, für Bau und Heimat hat Teile der Antwort zu den Fragen 4, 5, 5a, 5b, 6, 8c, 9 und 10 als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

2. Welche Haltung vertritt die Bundesregierung zur Frage, ob die CTG als informelles Gremium für die multilaterale Zusammenarbeit für den dort erledigten Datentausch einen formellen Rahmen oder einen Vertrag öffentlichen Rechts benötigt?

Der benötigte formelle Rahmen besteht in den gesetzlichen Rechtsgrundlagen der teilnehmenden Staaten aufgrund deren die nachrichtendienstliche Zusammenarbeit innerhalb der CTG erfolgt. Der Datenaustausch richtet sich dabei nach den jeweiligen einschlägigen nationalen Übermittlungsvorschriften. Die Errichtung gemeinsamer Dateien bzw. die Teilnahme an gemeinsamen Dateien erfolgt ebenfalls nach Maßgabe jeweiliger gesetzlicher nationaler Vorgaben.

3. Nach welcher Maßgabe kann nach Kenntnis der Bundesregierung im Rahmen der „operativen Plattform“ vereinbart werden, dass eingespeiste Daten nicht an beteiligte Behörden weitergeleitet werden, sondern nur an einzelne Teilnehmende?

Die „operative Plattform“ dient dem gemeinsamen Informationsaustausch. Wenn Informationen nicht für sämtliche Teilnehmer bestimmt sind, ist es nicht sachgerecht, sie in diesem Rahmen einzubringen, vielmehr wären sie dann sinnvollerweise gesondert mit den Partnern zu teilen, für die sie bestimmt sind.

4. Was ist der Bundesregierung dazu bekannt, dass die Datenbank im Herbst 2017 durch den AIVD umgebaut“ worden sein soll (http://gleft.de/2cf, bitte Details hierzu ausführen)?

Die Beantwortung der Frage 4 befindet sich in der als „VS – Nur für den Dienstgebrauch“ eingestuften Anlage.

a) Welche „systemtechnischen Vorkehrungen“ wurden zu der Datenbank getroffen, um die Richtigkeit und Vollständigkeit der Daten sicherzustellen?

Arbeitsmethoden und Vorgehensweisen der Nachrichtendienste des Bundes sind im Hinblick auf die künftige Aufgabenerfüllung besonders schutzwürdig.

Eine (zur Veröffentlichung bestimmte) Antwort der Bundesregierung auf diese Frage würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähigkeiten der Nachrichtendienste einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dabei würde die Gefahr entstehen, dass ihre bestehenden oder in der Entwicklung befindlichen operativen Fähigkeiten und Methoden aufgeklärt und damit der Einsatzerfolg gefährdet würde. Dies könnte einen Nachteil für die wirksame Aufgabenerfüllung der Nachrichtendienste und damit für die Interessen der Bundesrepublik Deutschland bedeuten.

Die erbetenen Informationen berühren derart schutzbedürftige Geheimhaltungsinteressen, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht ausnahmsweise überwiegt.

5. Welche Datenschutzbehörden oder Kontrollorgane (auch geheimdienstliche) haben sich nach Kenntnis der Bundesregierung mit der „operativen Plattform“ befasst, und welche Berichte haben diese erstellt?

   a) Inwiefern hat der niederländische Inlandsgeheimdienst AIVD nach Kenntnis der Bundesregierung hierfür Einsicht in die erforderlichen Unterlagen gewährt?

   b) Welche wesentlichen Defizite wurden bei diesen Prüfungen festgestellt?

Die Beantwortung der Fragen 5, 5a, 5b befindet sich in der als „VS – Nur für den Dienstgebrauch“ eingestuften Anlage.

6. Was ist der Bundesregierung darüber bekannt, inwiefern die „operative Plattform“ über eine Komponente zur Signalerfassenden Aufklärung (SIGINT) verfügt?

Die Beantwortung der Frage 6 befindet sich in der als „VS – Nur für den Dienstgebrauch“ eingestuften Anlage.

7. Wer ist aus Sicht der Bundesregierung für die „operative Plattform“ verantwortlich, und welche nationalen Datenschutzgrundsätze gelten für die Einrichtung und den Betrieb der Datenbank?

Die Verantwortlichkeit für die Teilnahme an der „operative Plattform“ liegt bei jedem Teilnehmer. Ergänzend wird auf die Antwort zu Frage 2 verwiesen.

Für den technischen Betrieb der Datenbank trägt die dateibetreibende Stelle, der niederländische Inlandsgeheimdienst AIVD, die Verantwortung. Für die in der Datenbank eingestellten Daten tragen die jeweils speichernden Dienste die entsprechende datenschutzrechtliche Verantwortung hinsichtlich der Zulässigkeit der Speicherung sowie der Richtigkeit, der Berichtigung, Löschung und Einschränkung der Verarbeitung der Daten. Für die zweckgemäße Nutzung der Daten ist hingegen der jeweilige datenabrufende Dienst verantwortlich. Die Teilnahme des BfV richtet sich nach § 22c Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (BVerfSchG).

   a) Welcher gemeinsame Rahmen für den Datenschutz wurde für die Datenbank vereinbart?

Entsprechend § 22c Satz 2 i. V. m. § 22b Absatz 5 BVerfSchG sind vor Beginn der Zusammenarbeit deren Ziele und das Nähere der Datenverwendung, insbesondere der Zweck der Datei und die Voraussetzungen der Verwendungen der Daten, zwischen den teilnehmenden Nachrichtendiensten zur Gewährleistung eines angemessenen Datenschutzniveaus und zum Ausschluss unangemessener Verwendung schriftlich vereinbart worden. Die Vereinbarung schließt die Zusage ein, die Daten ohne Zustimmung des eingebenden Dienstes nicht für einen anderen Zweck als den des festgelegten Dateizwecks zu verwenden oder an Dritte zu übermitteln.

b) Inwiefern teilt die Bundesregierung die Schlussfolgerung der niederländischen Kommission für die Überwachung der Nachrichten- und Sicherheitsdienste (CTIVD), wonach der AIVD „faktischer Geschäftsführer“ der Datenbank ist, jedoch alle teilnehmenden Geheimdienste für die Qualität und die Einhaltung des Datenschutzes verantwortlich sind und hierfür sogar eine „gesamtschuldnerische Haftung“ gilt?

c) Sofern die Bundesregierung keine gesamtschuldnerische Haftung“ sieht, wer ist aus ihrer Sicht für etwaige rechtliche Verstöße bei Einrichtung und dem Betrieb der Datenbank verantwortlich?

d) Sofern die Bundesregierung eine „gesamtschuldnerische Haftung“ nicht ausschließen will, welche Eckpunkte kann sie hierzu skizzieren?

Die Fragen 7b bis 7d werden zusammen beantwortet.

Wie in der Antwort zu Frage 7 ausgeführt, ist der AIVD für den technischen Betrieb der Datenbank verantwortlich.

Im Hinblick auf die Verantwortung für die Qualität und die Einhaltung des Datenschutzes gelten die in der Antwort zu Frage 7 dargestellten datenschutzrechtlichen Verantwortlichkeiten der an der Datenbank beteiligten Dienste. Angesichts der Differenzierung dieser Verantwortlichkeiten kann es keine „gesamtschuldnerische Haftung“ der teilnehmenden Dienste geben.

8. Welche Vereinbarungen über den Austausch, die Speicherung und die Verarbeitung der Daten sowie die Befugnisse und Pflichten jeder beteiligten Partei wurden bei der Einrichtung der Datenbank der „operativen Plattform“ beschlossen?

Auf die Antwort zu Frage 7a wird verwiesen.

a) Inwiefern entsprechen diese Vereinbarungen aus Sicht der Bundesregierung den Kriterien der Europäischen Menschenrechtskonvention (EMRK)?

Die Teilnahme des BfV richtet sich nach § 22c BVerfSchG, wodurch zugleich die Anforderungen der EMRK gewährleistet sind.

b) Welche gemeinsamen Garantien für einen angemessenen Rechtsschutz wurden hierfür festgelegt?

Der Rechtsschutz gegen Verwaltungshandeln des BfV richtet sich nach deutschem Recht bzw. dem jeweiligen nationalen Recht der teilnehmenden Dienste und bedarf keiner gemeinsamer Garantien.

c) Nach welchen Kriterien wird eine Person in die Datenbank aufgenommen?

Die Beantwortung der Frage 8c befindet sich in der als „VS – Nur für den Dienstgebrauch“ eingestuften Anlage.

d) Welche gemeinsamen Kriterien gelten für den Austausch von Daten über Minderjährige?

Es wird auf die Antwort zu Frage 2 verwiesen. Das BfV darf im Übrigen personenbezogene Daten in der gemeinsamen Datenbank gemäß § 22c Satz 2 i. V. m § 22b Absatz 6 BVerfSchG nur unter den Voraussetzungen des § 10 Absatz 1 und 3 § 11 Absatz 1 Satz 2 eingeben. Somit ist eine Speicherung von Daten oder über das Verhalten Minderjähriger vor Vollendung des 14. Lebensjahres in der Datenbank unzulässig.

e) Wie wird die Richtigkeit und Zuverlässigkeit der gespeicherten Daten gewährleistet?

Das BfV darf nach § 22c Satz 2 i. V. m. § 22b Absatz 6 BVerfSchG personenbezogene Daten in die gemeinsame Datei entsprechend § 10 Absatz 1 und 3, § 11 Absatz 1 eingeben, wenn es die Daten allen teilnehmenden ausländischen Nachrichtendiensten übermitteln darf.

Vor der Speicherung in die Datenbank führt das BfV eine umfassende Prüfung nach § 19 Absatz 3 BVerfSchG durch. Für eine Speicherung in dieser Datenbank gelten dieselben gesetzlichen Vorgaben wie für eine Speicherung in nationalen Datenbanken.

f) Auf welche Weise wird überprüft, ob die Daten nicht aus militärischen Quellen stammen oder anderweitig rechtswidrig erhoben oder gespeichert werden?

Es wird auf die Antwort zu Frage 2 verwiesen.

g) Welche Vereinbarungen wurden zur Weitergabe von Daten aus der „operativen Plattform“ gegenüber Dritten getroffen?

Daten, die in der Datenbank gespeichert werden, unterliegen der „Third-Party-Rule“ und dürfen nur mit Zustimmung des Nachrichtengebers weitergegeben werden.

h) Welche Verbesserungsmöglichkeiten sieht die Bundesregierung hinsichtlich des Austauschs, der Speicherung und der Verarbeitung der Daten in der „operativen Plattform“?

Arbeitsmethoden und Vorgehensweisen der Nachrichtendienste des Bundes sind im Hinblick auf die künftige Aufgabenerfüllung besonders schutzwürdig.

Eine (zur Veröffentlichung bestimmte) Antwort der Bundesregierung auf diese Frage würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähigkeiten der Nachrichtendienste einem nicht eingrenzbaren Personenkreis nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dabei würde die Gefahr entstehen, dass ihre bestehenden oder in der Entwicklung befindlichen operativen Fähigkeiten und Methoden aufgeklärt und damit der Einsatzerfolg gefährdet würde.

Es könnten entsprechende Abwehrstrategien entwickelt werden. Dies könnte einen Nachteil für die wirksame Aufgabenerfüllung der Nachrichtendienste und damit für die Interessen der Bundesrepublik Deutschland bedeuten.

Die erbetenen Informationen berühren derart schutzbedürftige Geheimhaltungsinteressen, dass das Staatswohl gegenüber dem parlamentarischen Informationsrecht ausnahmsweise überwiegt.

9. Welche Vereinbarung existiert über die Gruppe von Personen, denen der Zugang zur „operativen Plattform“ bzw. der angebundene Datenbank gewährt wird?

Die Beantwortung der Frage 9 befindet sich in der als „VS – Nur für den Dienstgebrauch“ eingestuften Anlage.

10. Nach welcher Maßgabe sind die nationalen (insbesondere die niederländischen) Zugangsberechtigungen zur „operativen Plattform“ bzw. der angebundenen Datenbank geregelt?

Die Beantwortung der Frage 10 befindet sich in der als „VS – Nur für den Dienstgebrauch“ eingestuften Anlage.

11. Welche Haltung vertritt die Bundesregierung zur Frage, welche Datenschutzbehörden oder Kontrollorgane für die Aufsicht der „operativen Plattform“ bzw. der angebundenen Datenbank zuständig sind oder sein sollten?

Angesichts der eigenständigen datenschutzrechtlichen Verantwortung der teilnehmenden Dienste auf der Grundlage ihrer jeweiligen nationalen Rechtsgrundlagen liegt die Zuständigkeit bei den betroffenen nationalen Datenschutzbehörden oder Kontrollorganen.

a) Inwiefern arbeiten diese Aufsichtsbehörden bzw. Kontrollorgane nach Kenntnis der Bundesregierung zusammen?

b) Nach welcher Maßgabe dürfen sich die Aufsichtsbehörden bzw. Kontrollorgane über gefundene Defizite austauschen?

Die Frage 11a und 11b werden zusammen beantwortet.

Über die Art der Zusammenarbeit der nationalen Datenschutzbehörden (bzw. Kontrollorgane) liegen der Bundesregierung keine Informationen vor. In jedem Fall richtet sich eine (mögliche) Zusammenarbeit nach dem jeweils anzuwendenden nationalen Recht.

c) Welche Haltung vertritt die Bundesregierung zur Forderung der CTIVD, dass entsprechende Einschränkungen zum Austausch über gefundene Defizite aufgehoben werden müssten?

Im deutschen Recht bestehen keine Einschränkungen, die zur Gewährleistung einer effektiven Datenschutzkontrolle des BfV aufzuheben wären. Es ist nicht ersichtlich, inwiefern – hier nicht bekannte – Einschränkungen in anderen Ländern zur Information über eine dort zu dortigen Behörden durchgeführte Datenschutzkontrolle die Effektivität der Datenschutzkontrolle in Deutschland beeinträchtigen könnte.

12. Welche Haltung vertritt die Bundesregierung zur Frage, ob einzelne nationale Aufsichtsbehörden bzw. Kontrollorgane mit bestimmten Aufgaben betraut werden könnten (etwa eine regelmäßige Kontrolle der Qualität der Daten oder die Einhaltung ihrer maximalen Speicherfrist)?

Auf die Antwort zu Frage 2 wird verwiesen. Im Übrigen stellt sowohl die Tätigkeit deutscher Nachrichtendienste als auch deren Kontrolle durch Aufsichtsbehörden, Gerichte und den Deutschen Bundestag die Ausübung von Staatsgewalt im Sinne von Artikel 20 Absatz 2 des Grundgesetzes (GG) dar. Eine Übertragung von Kontrollbefugnissen gegenüber deutschen Nachrichtendiensten und damit von hoheitlichen Aufgaben auf Behörden fremder Staaten würde daher im Konflikt mit dem Demokratieprinzip stehen.

13. Nach welcher Maßgabe hält die Bundesregierung auch eine übergeordnete, internationale Aufsicht für umsetzbar?

Auf die Antwort zu Frage 12 wird verwiesen.

14. Welche Erkenntnisse hat das Bundesamt für Verfassungsschutz (BfV) nach Bekanntwerden von Durchsuchungen beim österreichischen Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) erlangt, nachdem eine offizielle Anfrage an das BVT gestellt wurde, um Informationen darüber zu erhalten, „ob und ggf. welche Daten des BfV“ dabei abgeflossen sein könnten, was von der dortigen rechts-konservativen Regierung zwar sofort bestritten wurde („Justiz: Keine BVT-Daten aus Deutschland sichergestellt“, kurier.at vom 22. März 2018), von Medien in Österreich jedoch anderslautend berichtet wird („BVT-Affäre: Auslandsgeheimdienste in Aufruhr“, die presse.com vom 30. März 2018)?

a) Was hat die Prüfung ergeben, „wie die Kooperation mit dem BVT in Zukunft fortgesetzt werden kann“, bzw. wann soll diese Prüfung erfolgen (Antwort der Bundesregierung auf die Schriftliche Frage 19 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 19/1377)?

Die Fragen 14 und 14a werden zusammen beantwortet.

Nach jetzigem Stand liegen dem BfV keinerlei Kenntnisse vor, ob und ggf. welche Daten des BfV bei Durchsuchungen abgeflossen sein könnten. Darüber hinaus liegen der Bundesregierung keine weiteren Informationen vor. Eine weitere Stellungnahme oder Bewertung zum Sachverhalt erfolgt daher derzeit nicht.

15. Was ist der Bundesregierung darüber bekannt, inwiefern das Schengener Informationssystem (SIS II) zukünftig über Möglichkeiten zur Datenanalyse verfügen soll?

Hierzu liegen der Bundesregierung keine Informationen vor.

16. Welchen Fortgang nahm nach Kenntnis der Bundesregierung die Diskussion um die Einrichtung einer „Kriminalitätsinformationszelle“ zur Verfolgung des „Migrantenschmuggels“, die mit zehn Beamten aus dem Bereich der Strafverfolgung bei der Militärmission EUNAVFOR MED auf einem italienischen Flugzeugträger angesiedelt werden sollte, deren Ausgestaltung aber Gegenstand weiterer Verhandlungen und Beratungen im Politischen und Sicherheitspolitischen Komitee (PSK) sein soll (Antwort der Bundesregierung zu Frage 12 der Kleinen Anfrage auf Bundestagsdrucksache 19/647)?

17. Wo ist die „Kriminalitätsinformationszelle“ angesiedelt, und welches Personal arbeitet dort mit?

Die Fragen 16 und 17 werden gemeinsam beantwortet.

Nach weiteren Beratungen im Politischen und Sicherheitspolitischen Komitee und der Ratsarbeitsgruppe RELEX hat der Rat am 14. Mai 2018 mit der Anpassung des Ratsbeschlusses von EUNAVFOR MED Operation SOPHIA die Einrichtung einer sogenannten „Kriminalitätsinformationszelle“ (Crime Information Cell – CIC) beschlossen. Die CIC soll für eine sechsmonatige Projektphase auf dem Führungsschiff der Operation eingerichtet werden und bis zu zehn Mitglieder umfassen, die sich in erster Linie aus Angehörigen der EU Agenturen im Bereich Justiz- und Inneres, aber auch aus Personal nationaler Strafverfolgungsbehörden, zusammensetzen können.

a) Welche Fragen hatte die Bundesregierung nach Anmeldung eines Prüfvorbehaltes zum Vorschlag der „Kriminalitätsinformationszelle“ geprüft, und welches Ergebnis kann sie hierzu mitteilen (Antwort der Bundesregierung zu Frage 15 der Kleinen Anfrage auf Bundestagsdrucksache 19/353)?

Wie die Bundesregierung bereits in ihrer Antwort zu Frage 2 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/353 dargestellt hat, müssen die relevanten datenschutzrechtlichen Bestimmungen und unterschiedlichen Mandate und Rechtsgrundlagen der beteiligten Akteure beachtet werden. Die Bundesregierung hat dies im Rahmen der Gremienbefassung sichergestellt und deshalb der Einrichtung der CIC für die Projektphase zugestimmt.

b) Inwiefern wird nach Kenntnis der Bundesregierung die „Kriminalitätsinformationszelle“ mit dem „Migrant Smuggling Information Clearing House“ bei Europol zuarbeiten?

Europol ist eine der EU Agenturen aus dem Bereich Justiz und Inneres, mit denen der Informationsaustausch der EUNAVFOR MED Operation SOPHIA durch Einrichtung der CIC gemäß dem geltenden rechtlichen Rahmen verstärkt werden sollen. Das „Migrant Smuggling Information Clearing House“ wird dabei eine der Schnittstellen zwischen Europol und der CIC sein. Darüber hinaus wird auf die Antworten der Bundesregierung zu Frage 14 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/353 sowie zu Frage 12c der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/647 verwiesen.

18. An welchen Treffen des Rates für Justiz und Inneres der Europäischen Union oder des Ständigen Ausschusses für die operative Zusammenarbeit im Bereich der inneren Sicherheit (COSI) haben die CTG bzw. die „operative Plattform“ nach Kenntnis der Bundesregierung bislang teilgenommen?

Eine Übersicht über die Teilnahme der CTG an den Treffen des Rates für Justiz und Inneres (J/I-Rat) bzw. des COSI wird von der Bundesregierung nicht geführt.

Nach Kenntnis der Bundesregierung nahm der CTG-Vorsitz in der jüngeren Vergangenheit am 9. Juni 2017, am 12. Oktober 2017 und am 7. Dezember 2017 an Treffen des Rates für Justiz und Inneres teil.

Im Übrigen wird auf die Antwort der Bundesregierung zu Frage 30 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/9323, die Antwort der Bundesregierung zu Frage 19 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/9974 sowie die Antwort der Bundesregierung zu Frage 4 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/10641 verwiesen.

19. Welche Maßnahmen oder Projekte zur Stärkung der Zusammenarbeit zwischen Europol und der CTG bzw. entsprechende Vorschläge sind der Bundesregierung bekannt?

a) Welche neuen Zusammenarbeitsformen zwischen Europol und der CTG hätten aus Sicht der Bundesregierung einen operativen Mehrwert?

Die Fragen 19 und 19a werden zusammen beantwortet.

Die CTG ist ein informelles nachrichtendienstliches Gremium. Die Mitgliedsdienste unterliegen den jeweiligen nationalen gesetzlichen Vorgaben und haben unterschiedlich weitreichende Befugnisse. Möglichkeiten und Grenzen der Zusammenarbeit sind daher individuell von den Beteiligten zu definieren.

Für das BfV gilt: Im Rahmen der gesetzlichen Vorgaben übermittelt das BfV Informationen an das Bundeskriminalamt (BKA). Sofern für die dortige Aufgabenerfüllung als notwendig erachtet, nimmt das BKA in eigener Zuständigkeit einen Informationsaustausch mit Europol vor. Im Übrigen wird auf die Antwort der Bundesregierung zu den Fragen 1 und 1a der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/10641 verwiesen.

b) Welche Haltung vertritt die Bundesregierung zur Frage, inwiefern Geheimdienste in der Europol-Verordnung als „competent authority“ zu betrachten sind, mithin mit Europol Daten austauschen dürfen?

Artikel 2 Buchstabe a der Verordnung (EU) 2016/794 verweist auf die Zuständigkeiten nach dem jeweiligen nationalem Recht des Mitgliedstaates der Europäischen Union. Von abstrakten Rechtsprüfungen sieht die Bundesregierung ab.

c) Welche Haltung vertritt die Bundesregierung zur Frage, ob Europol und die CTG Verbindungsbeamte und Verbindungsbeamtinnen austauschen sollten bzw. dürfen?

Nach Artikel 23 Absatz 1 der Verordnung (EU) 2016/794 kann Europol, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, Kooperationsbeziehungen zu Unionseinrichtungen, den Behörden von Drittstaaten, internationalen Organisati-

onen und privaten Parteien herstellen und unterhalten. Die CTG erfüllt keine dieser Organisationsformen, so dass ein Austausch von Verbindungsbeamten oder -beamtinnen ausscheidet.

Im Übrigen wird auf die Antwort der Bundesregierung zu Frage 6 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/10641 verwiesen.

d) Inwiefern teilt der von Europol zum US-Projekt „Gallant Phoenix“ entsandte Verbindungsbeamte auch Daten mit den dort organisierten Geheimdiensten und Militärs, die von deutschen Behörden angeliefert wurden (Bundespolizei, BKA, BfV; siehe Antwort der Bundesregierung zu Frage 14 der Kleinen Anfrage auf Bundestagsdrucksache 19/647)?

Die Bundesregierung hat keine Erkenntnisse, dass der von Europol entsandte Verbindungsbeamte Daten mit Nachrichtendiensten oder Militärs im US-Projekt „Gallant Phoenix“ teilt.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.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