**Deutscher Bundestag** **Drucksache 19/21510**

**19. Wahlperiode** 06.08.2020

# Antwort

**der Bundesregierung**

**auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Fraktion DIE LINKE.**
**– Drucksache 19/21256 –**

## Schlussfolgerungen der Bundesregierung aus den Tätigkeitsberichten und Empfehlungen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Vorbemerkung der Fragesteller

Der Datenschutz in Deutschland ist zahlreichen Einschränkungen und Bedrohungen ausgesetzt. In seinem 28. Tätigkeitsbericht drückt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) seine Besorgnis darüber aus, dass in den vergangenen Jahren eine Vielzahl neuer Eingriffsbefugnisse für Sicherheitsbehörden beschlossen worden sei, die bereits zuvor bestehenden Kompetenzen dieser Behörden jedoch nicht evaluiert worden seien. Der BfDI kommt zu dem Schluss, dass die „konstante Akkumulation sicherheitsbehördlicher Eingriffsmöglichkeiten äußerst kritisch“ zu bewerten sei und empfiehlt ein „Sicherheitsgesetzmoratorium“ sowie die Einleitung eines Evaluationsprozesses der sicherheitsbehördlichen Eingriffskompetenzen.

Der BfDI stellt zudem eine Reihe von Kontrolllücken sowie datenschutzrechtlicher Verstöße durch Behörden des Bundes fest – zum Teil handelt es sich um die gleichen Verstöße und Lücken, auf die auch schon in früheren Tätigkeitsberichten hingewiesen wurde.

Unzureichende Datenschutzregeln gebe es beispielsweise bei den Geheimdiensten: Diesen gegenüber hat der BfDI keinerlei Sanktionsbefugnisse, wenn er rechtswidrige Verarbeitung personenbezogener Daten feststellt. Es bleibt lediglich der Rechtsweg der einzelnen Betroffenen, was nach Darlegung des BfDI „bei den ohnehin eingeschränkten Rechtsschutzmöglichkeiten der Betroffenen faktisch aber nur sehr schwierig erreichbar ist“. Die datenschutzkonforme Verwendung von Daten, die vom Bundesamt für Verfassungsschutz (BfV) oder vom Bundesnachrichtendienst (BND) in gemeinsam mit ausländischen Geheimdiensten geführte Dateien übertragen werden, kann vom BfDI ebenfalls nicht kontrolliert werden, da er die Daten nicht in diesen Dateien einsehen kann. Räume, in denen eine datenschutzrechtliche Kontrolle nicht möglich ist, sind aus Sicht der Fragestellerinnen und Fragesteller nicht hinzunehmen.

Das BfV handelt zudem nach Auffassung des BfDI ohne Rechtsgrundlage, wenn es Projektträger, die Förderanträge bei Bundesressorts stellen, überprüft,

---

*Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 5. August 2020 übermittelt.*
*Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.*

um etwaige Erkenntnisse über extremistische Bestrebungen an die jeweiligen Ressorts mitzuteilen.

Auch im Bereich der Bundespolizei sind die Befugnisse des BfDI nicht ausreichend, so hat er etwa – anders als im BKA-Gesetz (BKA = Bundeskriminalamt) geregelt – keine Abhilfebefugnisse bei rechtswidrigen Datenverarbeitungen der Bundespolizei (Quellen: Tätigkeitsbericht 2019 des BfDI).

1. Wie bewertetet die Bundesregierung die vom BfDI beschriebene datenschutzrechtliche Problematik des Fehlens von Sanktionsbefugnissen des BfDI im Bereich der Geheimdienste (bitte begründen)?

   Inwiefern hält sie die Einleitung gesetzgeberischer Schritte für angebracht mit dem Ziel, dem BfDI solche Sanktionsbefugnisse auch im Bereich der Geheimdienste zu erteilen, um den Schutz der Bürgerinnen und Bürger vor möglicher rechtswidriger Verarbeitung ihrer Daten zu erhöhen (bitte begründen), und was will sie ggf. konkret unternehmen?

Die Bundesregierung hält die am 25. Mai 2018 in Kraft getretene Regelung in § 16 Absatz 2 des Bundesdatenschutzgesetzes (BDSG) grundsätzlich für sachgerecht.

2. Wie bewertet die Bundesregierung die vom BfDI aufgezeigte Problematik des Fehlens von Abhilfebefugnissen des BfDI gegenüber der Bundespolizei (bitte begründen)?

   Inwiefern hält sie die Einleitung gesetzgeberischer Schritte für angebracht mit dem Ziel, im Bundespolizeigesetz solche Abhilfebefugnisse aufzunehmen, die zumindest den im neuen Bundeskriminalamtsgesetz enthaltenen Befugnissen entsprechen, und was will sie ggf. konkret unternehmen?

Die Bundesregierung beabsichtigt die Aufnahme von entsprechenden Abhilfebefugnissen des BfDI gegenüber der Bundespolizei bei rechtswidrigen Datenverarbeitungen im Rahmen des Entwurfs einer Novelle des Bundespolizeigesetzes.

3. Inwiefern beabsichtigt die Bundesregierung, sich für eine Abschaffung der Antiterrordatei einzusetzen (bitte begründen)?

   a) Trifft es zu, dass Vertreter von Sicherheitsbehörden eine solche Abschaffung befürworten, weil die Datei zu wenig Nutzen biete (https://www.spiegel.de/politik/warum-bka-und-verfassungsschutz-die-antiterrordatei-abschaffen-wollen-a-00000000-0002-0001-0000-000161665848), und wenn ja, wie positioniert sich die Bundesregierung dazu?

Die Fragen 3 und 3a werden gemeinsam beantwortet.

Das Ziel der (ersatzlosen) Abschaffung der Antiterrordatei (ATD) wird durch die Bundesregierung weder beabsichtigt noch verfolgt. Ihrer Einschätzung zufolge ist die Bedrohungslage im Bereich des internationalen Terrorismus nach wie vor unverändert hoch.

Im Übrigen wird auf die Antwort der Bundesregierung zu den Fragen 9, 10 und 11 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/11031 verwiesen.

b) Welche Angaben zur Nutzung der Antiterrordatei in den Jahren 2018 und 2019 kann die Bundesregierung machen?

Die nachstehende Tabelle zeigt die Nutzung der ATD im Jahr 2019.

| | **Personenerfassungen ATD 2019** | **Personensuchanfragen ATD 2019** |
|---|---|---|
| Polizei Bund | 687 | 16.827 |
| Polizei Land | 440 | 19.373 |
| Dienste Bund | 450 | 1.982 |
| Dienste Land | 66 | 617 |
| **Gesamt** | **1.643** | **38.799** |

Im Übrigen wird auf die Antwort der Bundesregierung zu den Fragen 1, 3 und 5 der Kleinen Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/11031 wird verwiesen.

c) Inwiefern hält die Bundesregierung die Antiterrordatei für ein wirksames und erforderliches Instrument der Sicherheitspolitik, und nach welchen Kriterien bemisst sie dies?

Nach § 1 des Antiterrordateigesetzes (ATDG) dient die ATD den Sicherheitsbehörden von Bund und Ländern bei der Erfüllung ihrer jeweiligen gesetzlichen Aufgaben zur Aufklärung oder Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland. Erkenntnisse aus der ATD dienen insbesondere dem Zweck der Kontaktanbahnung zwischen den teilnehmenden Behörden zur Stellung von Ersuchen um Übermittlung von Erkenntnissen zur Wahrnehmung ihrer jeweiligen Aufgabe zur Aufklärung oder Bekämpfung des internationalen Terrorismus.

Nach Auffassung der Bundesregierung verfügt die ATD aufgrund ihrer Eigenschaft als eine gemeinsam genutzte, zentral geführte, standardisierte Datei mit bestimmten, gesetzlich festgelegten Datenkategorien über die Voraussetzungen, eine solche Kontaktanbahnung zu ermöglichen und die Zusammenarbeit zwischen Polizeien und Nachrichtendiensten auf Bundes- und Landesebene damit zu vereinfachen.

Im Übrigen wird auf die Antwort zu den Fragen 3 und 3a verwiesen.

4. Wie positioniert sich die Bundesregierung zur Besorgnis des BfDI, dass mit der in den vergangenen Jahren beschlossenen Vielzahl neuer Eingriffsbefugnisse für die Sicherheitsbehörden kein Trend einer parallelen Evaluierung der bereits bestehenden Kompetenzen dieser Behörde korrespondiere, und die „konstante Akkumulation sicherheitsbehördlicher Eingriffsmöglichkeiten äußerst kritisch“ zu bewerten sei?

   a) Inwiefern und bei welchen Behörden beabsichtigt die Bundesregierung, bis wann eine Evaluation der bestehenden Eingriffsbefugnisse durchzuführen (bitte möglichst Details nennen)?

   b) Inwiefern hält die Bundesregierung ein Moratorium bei der Verabschiedung neuer Sicherheitsgesetze für angebracht, zumindest bis zum Abschluss einer solchen Evaluation (bitte begründen)?

Die Fragen 4 bis 4b werden gemeinsam beantwortet.

Eine Vielzahl nachrichtendienstlicher Regelungen unterliegt speziellen periodischen Berichtspflichten, die auch der laufenden Evaluierung dienen (z. B.: § 8b Absatz 3, § 9 Absatz 4 Satz 7, § 9b Absatz 1 Satz 2, § 17 Absatz 3 Satz 6, § 18 Absatz 1a Satz 4 des Bundesverfassungsschutzgesetzes – BVerfSchG, § 3 Absatz 1 Satz 3, § 5 Satz 2, § 24 Absatz 2 Satz 2 des Bundesnachrichtendienstgesetzes – BNDG, § 14 Absatz 1 des Artikel 10-Gesetzes – G 10). Eine Analyse der Regelungserfordernisse erfolgt überdies im Rahmen der Arbeiten an neuen Gesetzgebungsvorhaben. Grundrechtseinschränkende Gesetze dürfen nur erlassen werden, wenn sie zur Erreichung eines legitimen Regelungszwecks geeignet, erforderlich und angemessen sind.

5. Inwiefern setzt sich die Bundesregierung dafür ein, dass die datenschutzrechtlichen Einwände bzw. Bedenken des Europäischen Datenschutzausschusses und des BfDI in Bezug auf die Verhandlungen über die Anwendung des „Cloud Act“ zwischen den USA und der Europäischen Union berücksichtigt werden?

   a) Teilt sie die Bedenken des BfDI, dass direkte Datenübermittlungen an US-Strafverfolgungsbehörden „außerhalb des Rechtshilfeweges nur sehr begrenzt mit der DSGVO (Datenschutz-Grundverordnung) vereinbar“ sind, wenn nein, warum nicht, wenn ja, welche Schlussfolgerungen zieht sie daraus?

   b) Setzt sie sich konkret dafür ein, dass Datenübermittlungen auch künftig die Einhaltung des bestehenden Rechtshilfeweges voraussetzen, und ist dieser Punkt für sie entscheidend, wenn nein, warum nicht?

Die Fragen 5 bis 5b werden gemeinsam beantwortet.

Die Bundesregierung teilt die Ansicht, dass es zwischen den Regelungen des US-Cloud Act und der Datenschutzgrundverordnung zu Rechtskonflikten kommen kann.

Der Rat hat der EU-Kommission im Juni 2019 ein Mandat zur Aufnahme von Verhandlungen mit den USA betreffend ein Abkommen über den Zugang zu elektronischen Beweismitteln erteilt. Die Bundesregierung unterstützt die Verhandlungen der Europäischen Kommission mit den USA über ein Abkommen, weil das geplante Abkommen auch aus Sicht der Bundesregierung eine sinnvolle Ergänzung des neuen europäischen Rechtsrahmens zu E-Evidence sein wird.

Die Bundesregierung setzt sich für einen hohen Grundrechtsschutz und wirksame Rechtsschutzmechanismen ein. Sie ist der Ansicht, dass der Schutzstandard, den sich die Mitgliedstaaten der Europäischen Union untereinander mit dem neuen Rechtsrahmen zu E-Evidence setzen wollen, auch gegenüber Drittstaaten gelten sollte. Dies gilt auch mit Blick auf eventuelle Notifikationsverpflichtungen des Anordnungsstaates, für die sich die Bundesregierung im Zuge der Verhandlungen zur EPOC-Verordnung eingesetzt hat.

6. Wie positioniert sich die Bundesregierung zum Verordnungsverschlag der Europäischen Kommission bezüglich „e-Evidence“, wonach europäische Strafverfolgungsbehörden Bestands-, Verkehrs- und Inhaltdaten unmittelbar bei Providern von Telekommunikations- und Internetdienstleistungen in anderen EU-Mitgliedstaaten erheben können sollen?

   a) Welche datenschutzrechtlichen Probleme sieht sie bei diesem Vorschlag, und was will sie unternehmen, um diesen abzuhelfen?

b) Inwiefern teilt sie die datenschutzrechtliche Besorgnis des BfDI und dessen Auffassung, es sollte „nicht allein den Providern überlassen bleiben, die Rechtmäßigkeit einer Anordnung zu überprüfen“?

c) Inwiefern will sie sich dafür einsetzen, dass die Justizbehörden der beteiligten Mitgliedstaaten zwingend parallel unterrichtet werden müssen?

Die Fragen 6 bis 6c werden gemeinsam beantwortet.

Die Bundesregierung unterstützt grundsätzlich das Ziel, geeignete Instrumente zur beschleunigten und verbesserten grenzüberschreitenden Gewinnung elektronischer Beweismittel in Strafverfahren zu schaffen.

Jedoch ist auch in diesem Dossier ein angemessenes Grundrechts- und Rechtsschutzniveau sicherzustellen. Die Bundesregierung hatte sich – gemeinsam mit anderen Mitgliedstaaten der Europäischen Union – im Zuge der Verhandlungen zur EPOC-VO engagiert dafür eingesetzt, dass der Mitgliedstaat, in dem der angefragte Provider seinen Sitz hat, zumindest bei der Abfrage von Verkehrs- und Inhaltsdaten über die Herausgabeanordnung unterrichtet wird und der Anordnung im begründeten Einzelfall (insbesondere bei grundrechtlichen Bedenken) auch widersprechen kann.

Die Mehrheit der Mitgliedstaaten entschied jedoch, dass die Unterrichtung des jeweiligen Vollstreckungsstaates nur bei Inhaltsdaten zu erfolgen hat und es kein Vetorecht geben solle, sondern die Entscheidung über ein Aufrechterhalten der Europäischen Herausgabeanordnung im Ermessen des Anordnungsstaates verbleiben solle (siehe Artikel 5 Absatz 7 und Artikel 7a der EPOC-VO in der Fassung der Allgemeinen Ausrichtung). Für die Bundesregierung war unter anderem dies ein Grund dafür, bei der Abstimmung über die EPOC-VO im Rat der Justiz- und Innenminister vom Dezember 2018 mit „Nein“ zu stimmen.

Das Dossier befindet sich nach wie vor in den Beratungen des EP (federführender Ausschuss: Ausschuss für bürgerliche Freiheiten, Justiz und Inneres – LIBE, Berichtsentwurf liegt seit November 2019 vor); eine finale Positionierung steht aus. Inwieweit diese Lösung im Trilog noch Veränderungen erfährt, bleibt abzuwarten.

7. Wie positioniert sich die Bundesregierung zum derzeit verhandelten zweiten Zusatzprotokoll zur sog. Cybercrime-Konvention, das die direkte grenzüberschreitende Erhebung durch Strafverfolgungsbehörden bei Providern in anderen Staaten regelt, und inwiefern teilt sie die datenschutzrechtliche Besorgnis des BfDI, der darauf hinweist, dass in den Unterzeichnerstaaten „eine Vielfalt von teilweise sehr unterschiedlichen Rechtssystemen und Datenschutzstandards existieren“?

   Inwiefern will sie sich im Rahmen der EU dafür einsetzen, den datenschutzrechtlichen Problemen abzuhelfen?

Für das derzeit im Rahmen des Europarats verhandelte Zweite Zusatzprotokoll zum Übereinkommen über Computerkriminalität (sog. Budapest Convention), welches eine stärkere Zusammenarbeit bei der Sicherung elektronischer Beweismittel und der Verfolgung von Computerkriminalität zum Ziel hat, hat der Rat der Europäischen Union der Europäischen Kommission im Juni 2019 ein Verhandlungsmandat erteilt. Danach soll die Kommission auch sicherstellen, dass das Zusatzprotokoll im Einklang mit EU-Recht und somit auch mit dem europäischen Datenschutzrecht steht. Die Kommission hat sich daher in den bisherigen Verhandlungen für Regelungen zu geeigneten und effektiven Kontrollmechanismen im Zusatzprotokoll zur Gewährleistung des europarechtlich gebotenen Schutzniveaus eingesetzt.

Die Bundesregierung unterstützt die Arbeiten an dem Zweiten Zusatzprotokoll zur Budapest Konvention wie auch die Position der Kommission, die europäischen Datenschutzstandards darin umzusetzen.

8. Warum ist nach Kenntnis der Bundesregierung der BfDI nicht mehr zu Terminen des Bundesministeriums des Innern, für Bau und Heimat (BMI) zur Erprobung des „Datenhauses“ im Rahmen des Projektes „Polizei 2020“ eingeladen worden, nachdem er erhebliche Einwände gegen das der Erprobung zugrunde liegende System geäußert hatte (vgl. den 28. Tätigkeitsbericht des BfDI)?

   a) Ist mittlerweile seine Einladung zu künftigen Erprobungen gewährleistet, und wenn nein, warum nicht?

Die Fragen 8 bis 8a werden gemeinsam beantwortet.

Das Bundesministerium des Innern, für Bau und Heimat (BMI), das Bundeskriminalamt (BKA) sowie die Bund-Länder-Gremien des Programms 2020 befinden sich im fortlaufenden Austausch mit dem BfDI zu den Inhalten des Programms Polizei 2020, einschließlich der Planungen zum Proof of Concept (PoC) Datenkonsolidierung. Der BfDI hat an der Sitzung der AG Recht des Programms Polizei 2020 am 19. Februar 2019 teilgenommen. Mit Schreiben vom 4. April und vom 19. Juni 2019 hat sich der BfDI zum PoC Datenkonsolidierung ausführlich gegenüber dem BKA geäußert. In Besprechungen mit dem BMI am 2. Dezember 2019 sowie mit Ländervertretern des Programms Polizei 2020 und mehreren Landesdatenschutzbeauftragten am 4. Februar 2020 hat er seine Auffassung zum PoC Datenkonsolidierung ebenfalls dargelegt.

   b) Inwiefern und in welchem Umfang sind die Einwände des BfDI vom BMI ernst genommen worden und in die Planungen eingeflossen?

Die Hinweise des BfDI sind sorgfältig geprüft worden und werden in die weiteren Überlegungen zum PoC Datenkonsolidierung einbezogen.

   c) Existiert inzwischen ein schriftliches Konzept zur datenschutzrechtlichen Prüfung, und wenn nein, warum nicht, wenn ja, was sieht dieses vor (bitte möglichst beilegen oder, falls eine Übermittlung an den Deutschen Bundestag verwehrt wird, zusammenfassen)?

Der BfDI wird regelmäßig zu den Planungen des Programms Polizei 2020 beteiligt (vgl. Antwort zu Frageteil 8a). Datenschutzrechtliche Fragen werden fortlaufend und entsprechend des jeweiligen Entwicklungsstands des Programms geprüft. Die Datenschutz-Folgenabschätzung wird nach Maßgabe der gesetzlichen Vorgaben erfolgen.

9. Wie positioniert sich die Bundesregierung zum Gutachten des Europäischen Gerichtshofes vom 26. Juli 2017 zum Fluggastdaten-Abkommen zwischen Kanada und der Europäischen Union, und welche Schlussfolgerungen sind aus ihrer Sicht hieraus für dieses und ähnliche Abkommen mit weiteren Staaten notwendig, und inwiefern setzt sich die Bundesregierung dafür ein?

Die Bundesregierung hat das Gutachten des Europäischen Gerichtshofs (EuGH) vom 26. Juli 2017 zum Fluggastdaten-Abkommen zwischen Kanada und der Europäischen Union zur Kenntnis genommen. Dem Gutachten des EuGH kommt eine wesentliche Bedeutung für die grundrechtskonforme Ausgestaltung dieses und vergleichbarer Abkommen zu.

Im Übrigen wird auf die Antworten der Bundesregierung zu Frage 4 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/5816 und zu Frage 5 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 19/15699 verwiesen.

10. Wie beurteilt die Bundesregierung unter dem Aspekt der Nutzerfreundlichkeit die derzeitigen Möglichkeiten von Bürgerinnen und Bürgern im Zusammenhang mit dem Onlinezugangsgesetz, die stattfindenden Datenverarbeitungsprozesse nachvollziehen und kontrollieren zu können, und inwiefern beabsichtigt sie, hier der Empfehlung des BfDI zu einer nutzerfreundlicheren Regelung nachzukommen (bitte begründen)?

Im Rahmen der Umsetzung des Onlinezugangsgesetzes (OZG) steht Nutzerfreundlichkeit im Fokus. Das umfasst auch das Thema Datenschutz. Der im Juni dieses Jahres veröffentlichte Servicestandard zur OZG-Umsetzung empfiehlt hierzu, dass bei der Verarbeitung von Daten und Informationen der Nutzerinnen und Nutzern in digitalen Angeboten Sicherheitsvorkehrungen zu ihrem Schutz getroffen und transparent gemacht werden. Außerdem sollen Datenaustausche zwischen Behörden durch zwischengeschaltete Intermediäre abgesichert und im Datencockpit der Nutzerin bzw. des Nutzers protokolliert werden. Das Datencockpit bietet eine nutzerfreundliche Lösung für die OZG-Umsetzung, die es Nutzerinnen und Nutzern ermöglicht nachzuvollziehen, welche Daten von der Verwaltung ausgetauscht und verarbeitet werden.

11. Wie positioniert sich die Bundesregierung derzeit zur Einführung von Videoüberwachung mit automatischer Gesichtserkennung, welche Projekte werden hierzu von Einrichtungen des Bundes oder mit deren Unterstützung durchgeführt oder geplant, und inwiefern hält die Bundesregierung eine spezielle Rechtsgrundlage für diese Technik für notwendig (bitte begründen)?

Die Meinungsbildung in der Bundesregierung zur Einführung von Videoüberwachung mit automatisierter Gesichtserkennung ist noch nicht abgeschlossen. Ein Test entsprechender Systeme wurde 2018 am Bahnhof Berlin Südkreuz abgeschlossen und die Ergebnisse veröffentlicht. Aktuell sind keine weiteren Projekte zur Live-Videoüberwachung mit Systemen zur Gesichtserkennung bei der Bundespolizei geplant. Für einen Einsatz entsprechender Systeme im Wirkbetrieb im Zuständigkeitsbereich der Bundespolizei ist zunächst die Schaffung einer Rechtsgrundlage erforderlich.

12. Beabsichtigt die Bundesregierung, gesetzgeberische Schritte einzuleiten, um eine klare Zuständigkeitsregelung für die Kontrolltätigkeit von BfDI und G10-Kommission zu schaffen, die auch die Kooperation zwischen diesen beiden Aufsichtsorganen umfasst?

Zuständigkeitsregelungen über Kontrolltätigkeit und Kooperation von BfDI und G 10-Kommission sind bereits in § 26a Absatz 2 BVerfSchG i. V. m. § 32 BNDG und § 15 Absatz 5 Sätze 4 G 10 getroffen. Auch in der Praxis findet anlassbezogen eine gute und erfolgreiche Kooperation zwischen der G 10-Kommission und dem BfDI statt.

13. Beabsichtigt die Bundesregierung gesetzgeberische Schritte einzuleiten, um die Kontrollbefugnis des BfDI umfassend auch beim Führen gemeinsamer Daten des BfV mit ausländischen Geheimdiensten anzuerkennen und diese ggf. gesetzlich klarstellend zu regeln?

    a) Sieht die Bundesregierung eine problematische Kontrolllücke darin, dass der BfDI die von deutscher Seite in einer vom einem ausländischen Geheimdienst geführten gemeinsamen Datei nicht dort, also in dieser Datei, sehen kann, und somit auch ihre Verarbeitung kontrollieren kann, sondern lediglich prüfen kann, welche Daten von BfV oder BND dorthin übertragen worden sind (bitte begründen), und welche Schlussfolgerungen zieht sie daraus?

Die Fragen 13 und 13a werden aufgrund des Sachzusammenhangs gemeinsam beantwortet. Die Bundesregierung geht davon aus, dass die Fragesteller in der Einleitungsfrage statt „Daten“ den Begriff „Dateien“ meinten.

Die Tätigkeit des BfV und des BND unterliegt in Bezug auf die Einhaltung der Vorschriften über den Datenschutz auch bei gemeinsamen Dateien der Kontrolle des BfDI. Die Tätigkeit ausländischer Nachrichtendienste bei der Datenverarbeitung in gemeinsamen Dateien unterliegt jeweils der Kontrolle von deren Datenschutzaufsichtsbehörden. Dadurch ist eine Kontrolle gewährleistet.

    b) Wie viele personenbezogene Daten zu wie vielen Personen haben BfV und BND im vergangenen Jahr in gemeinsamen Dateien mit ausländischen Geheimdiensten übertragen (falls der Bundesregierung diese Zahl nicht bekannt ist, bitte, soweit vorhanden, andere Angaben zum Umfang entsprechender Datenübertragungen machen)?

    c) In wie vielen gemeinsam vom BfV oder BND mit ausländischen Geheimdiensten geführten Daten werden wie viele personenbezogene Daten gespeichert?

Die Fragen 13b und 13c werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

§ 22b und § 22c BVerfSchG regeln die Voraussetzungen für eine Teilnahme des BfV an gemeinsamen Dateien mit ausländischen Nachrichtendiensten.

Das BfV nimmt im Rahmen des internationalen Informationsaustauschs an einer gemeinsamen Datenbank mit ausländischen Nachrichtendiensten im Bereich der Counter Terrorism Group (CTG) teil. Im BNDG treffen §§ 26 ff. BNDG Regelungen über gemeinsame Dateien mit ausländischen Nachrichtendiensten. Der BND ist an zwei gemeinsamen Dateien mit ausländischen Nachrichtendiensten beteiligt. Die Bundesregierung ist nach sorgfältiger Abwägung der in diesem Fall widerstreitenden Interessen zu der Auffassung gelangt, dass eine weitergehende Beantwortung nicht erfolgen kann. Die erbetenen Auskünfte zu der genauen Anzahl der ausgetauschten Daten sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die unter dem Aspekt des Schutzes der nachrichtendienstlichen Zusammenarbeit mit ausländischen Partnern besonders schutzbedürftig sind. Eine öffentliche Bekanntgabe von Informationen zur Arbeitsweise und Organisation von ausländischen Partnerdiensten und damit einhergehend die Kenntnisnahme durch Unbefugte hätte erhebliche nachteilige Auswirkungen auf die vertrauensvolle Zusammenarbeit.

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 der Sicherheitslage in der Bundesrepublik Deutschland sowie im Hinblick auf den Schutz deutscher Interessen im Ausland. Die künftige Aufgabenerfüllung des BfV und des BND würde stark beeinträchtigt. Dies würde für die Auftragserfüllung des BfV und des BND erhebliche Nachteile zur Folge ha-

ben und kann für die Interessen der Bundesrepublik Deutschland schädlich sein. Insofern könnte die Offenlegung entsprechender Informationen die Sicherheit der Bundesrepublik Deutschland gefährden oder ihren Interessen schweren Schaden zufügen.

Aus der sorgfältigen Abwägung der verfassungsrechtlich garantierten Informationsrechte des Deutschen Bundestages und seiner Abgeordneten mit den negativen Folgen für die künftige Arbeitsfähigkeit und Aufgabenerfüllung des BfV und des BND sowie den daraus resultierenden Beeinträchtigungen der Sicherheit der Bundesrepublik Deutschland folgt, dass auch eine eingestufte Übermittlung der Informationen nach Maßgabe der Geheimschutzordnung und damit einhergehende Einsichtnahme in der Geheimschutzstelle des Deutschen Bundestages ausscheidet. Die mit einer solchen Bekanntgabe verbundene Erhöhung der Anzahl der Geheimnisträger würde nämlich die Wahrscheinlichkeit des Bekanntwerdens, z. B. durch Ausspähung seitens nachrichtendienstlicher Gegner, erhöhen. Aus Gründen des Staatswohls kann eine solche – wenn auch geringe – Risikoerhöhung nicht in Kauf genommen werden.

14. In welchem Umfang werden personenbezogene Daten von öffentlichen Stellen des Bundes bei Versand per E-Mail ausschließlich verschlüsselt gesendet?

Die Bundesregierung führt keine Statistik über den Umfang von E-Mails mit personenbezogenen Daten, unabhängig davon, ob diese verschlüsselt oder unverschlüsselt versendet werden.

Grundsätzlich werden die Daten in Netzen des Bundes mit Transportverschlüsselung übertragen. Dies umfasst auch E-Mails. Sofern E-Mails an Adressaten außerhalb der Netze des Bundes versendet werden, erfolgt dies ebenfalls mittels Transportversschlüsselung, sofern der E-Mail-Server des Zieladressaten dies unterstützt. Ebenso akzeptieren die E-Mail-Server des Bundes eine Transportverschlüsselung für eingehende E-Mails.

Mit DE-Mail besteht zudem eine Möglichkeit für Dritte an die Verwaltung mittels verschlüsselter E-Mail heranzutreten.

a) Teilt die Bundesregierung die Auffassung des BfDI, ein unverschlüsselter Datenversand per E-Mail sei bei sensiblen Daten „auch dann nicht rechtmäßig, wenn vorher eine entsprechende Einwilligung des Empfängers eingeholt wurde, da diese in der Regel nicht datenschutzkonform erteilt werden kann“ (falls nein, bitte begründen)?

Die Frage wird im Hinblick auf die im Tätigkeitsbericht des BfDI angesprochene Vorschrift des § 87a der Abgabenordnung (AO) beantwortet. Mit § 87a Absatz 1 Satz 3 Halbsatz 2 AO erlaubt das geltende Recht den Finanzbehörden, auch Daten, die dem Steuergeheimnis unterliegen, unverschlüsselt elektronisch zu übermitteln, wenn alle betroffenen Personen schriftlich eingewilligt haben. Entsprechend der Begründung des Gesetzentwurfs (Bundestagsdrucksache 19/13436) ist darauf hinzuweisen, dass das Verschlüsselungsgebot letztlich der Wahrung des Steuergeheimnisses dient. Da das Steuergeheimnis eine Offenbarung mit Zustimmung des Betroffenen gestattet (§ 30 Absatz 4 Nummer 3 AO), ist es sachgerecht, eine unverschlüsselte Übermittlung nach § 30 AO geschützter Daten unter der Voraussetzung zuzulassen, dass alle betroffenen Personen in die unverschlüsselte Übermittlung schriftlich eingewilligt haben. Dies ist nicht zuletzt Ausdruck der „Datenherrschaft“ der betroffenen Person. Die betroffene Person muss vor Erteilung der Einwilligung über die Risiken der unverschlüsselten Übermittlung informiert werden. Außerdem muss die Einwilligung freiwillig erteilt werden, die Finanzbehörde muss also auch alternative Formen der

Datenübermittlung (z. B. Briefpost) ermöglichen. Zudem kann die Einwilligung jederzeit und ohne belastende Rechtswirkungen mit Wirkung für die Zukunft widerrufen werden.

b) Teilt die Bundesregierung die Auffassung des BfDI, nationale Vorschriften, die einen unverschlüsselten E-Mailversand legitimieren, seien nicht DSGVO-konform?

Die Bundesregierung teilt die dargestellte Auffassung nicht.

Im Übrigen wird auf die Antwort zu Buchstabe 14a verwiesen.

c) Welche Schlussfolgerungen zieht die Bundesregierung für den Fall, dass gegenwärtig noch personenbezogene Daten unverschlüsselt per E-Mail versandt werden?

Nach Artikel 32 Absatz 1 der Datenschutz-Grundverordnung (DSGVO) haben der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Im Hinblick auf die Versendung von E-Mails ist daher abhängig vom Risiko für die Rechte und Freiheiten der betroffenen Personen im Einzelfall zu bestimmen, in welchem Umfang eine Verschlüsselung der Kommunikation erforderlich ist.

15. Welche Schlussfolgerungen zieht die Bundesregierung aus der Kritik des BfDI, für die Überprüfung von Projektträgern, die Förderanträge bei Bundesressorts stellen, fehle es dem BfV an einer Rechtsgrundlage?

Das BMI, in dessen Geschäftsbereich das BfV angesiedelt ist, teilt die Auffassung, dass es einer Rechtsgrundlage für die Überprüfung von Projektträgern fehle, nicht.

16. Wie positioniert sich die Bundesregierung zur Empfehlung des BfDI, die Strafprozessordnung in Hinsicht auf die Erhebung und Nutzung von Daten, die von V-Leuten ermittelt wurden, zu überarbeiten und die Zusammenarbeit mit Verfassungsschutzbehörden enger und präziser zu regeln?

Der Einsatz von Vertrauenspersonen stützt sich auf §§ 161, 163 der Strafprozessordnung und berücksichtigt die Maßgaben der höhergerichtlichen Rechtsprechung.

Konkrete Einzelheiten zur Handhabung sind unter anderem in Anlage D der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) geregelt.

Das Bundesministerium der Justiz und für Verbraucherschutz hat ein Gutachten bei der Großen Strafrechtskommission des Deutschen Richterbundes in Auftrag gegeben, das inzwischen vorliegt. Deren Empfehlung, den Einsatz von Vertrauenspersonen und Informanten bereichsspezifisch gesetzlich zu regeln, wird derzeit unter Berücksichtigung der weiteren Diskussionsbeiträge aus Literatur und Praxis geprüft.

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