Deutscher Bundestag **Drucksache 18/7246**

18. Wahlperiode 13.01.2016

Antwort

der Bundesregierung

der Abgeordneten Andrej Hunko, Jan van Aken, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 18/7034 –

Austausch geheim eingestufter Informationen unter europäischen Geheimdiensten, Polizeien und Militärs

Vorbemerkung der Fragesteller

Als „Netzanwendung für den sicheren Informationsaustausch“ betreibt die EU-Polizeiagentur Europol seit dem 1. Juli 2009 eine „Secure Information Exchange Network Application“ (SIENA, Europol-Jahresbericht 2011). Das Instrument soll die „schnelle, sichere und nutzerfreundliche Kommunikation“ sowie den Austausch operativer und strategischer kriminalpolizeilicher Informationen und Erkenntnisse zwischen Europol, den Verbindungsbüros der Mitgliedstaaten und Dritten, die über Kooperationsabkommen mit Europol verfügen, ermöglichen (etwa Eurojust, INTERPOL, aber auch Australien, Kanada, Norwegen, die Schweiz und die USA). Laut der Europol-Webseite sind im vergangenen Jahr 573 Behörden und 4 722 Nutzende aus 28 Mitgliedstaaten vernetzt gewesen. Laut Europol seien 14 Dritte direkt und 19 weitere indirekt angeschlossen. 34 472 neue Fälle seien eröffnet worden, davon 4 Prozent von Dritten. Unter den fünf größten Tatkomplexen finden sich „Drogen“ und „illegale Einwanderung“.

Auch deutsche Behörden führen ihre Zugriffe auf Europols Informationssysteme mittels SIENA durch (Bundestagsdrucksache 16/9987). Hierzu zählen außer dem Bundeskriminalamt die Bundespolizei, der Zollfahndungsdienst und Staatsanwaltschaften.

1. Wer hat das SIENA-Netzwerk nach Kenntnis der Bundesregierung eingerichtet und zertifiziert?

Das SIENA-Netzwerk wurde von Europol eingerichtet und vom Europol Security Committee akkreditiert.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 12. Januar 2016 übermittelt.

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

2. Auf welche Weise und mit welchen Produkten werden in SIENA verteilte Nachrichten soft- und hardwareseitig verschlüsselt (bitte Produkt- und Herstellername angeben)?

Die Applikation SIENA nutzt Secure Sockets Layer (SSL) als Verschlüsselungsprotokoll. Die eingesetzte Hardware befindet sich im Eigentum von Europol. Produkt- und Herstellername sind der Bundesregierung nicht bekannt.

3. Welche über SIENA kommunizierenden polizeilichen oder geheimdienstlichen Arbeitsgruppen oder Netzwerke sind der Bundesregierung bekannt?

Im Rahmen des polizeilichen Informationsaustausches kommunizieren die Asset Recovery Offices der Mitgliedstaaten über SIENA. Ferner wurden SIENA-Postfächer für die Staatsschutzdienststellen der Mitgliedstaaten eingerichtet. Der Bundesregierung sind keine geheimdienstlichen Arbeitsgruppen oder Netzwerke bekannt, welche über SIENA kommunizieren.

4. Welchen weiteren Dritten wird gestattet, ebenfalls an SIENA teilzunehmen (bitte nach direkten und indirekten Anschlüssen darstellen)?

Folgende Drittstaaten und -stellen können nach Kenntnis der Bundesregierung mittels SIENA über einen direkten Anschluss kommunizieren:

Albanien, Australien, Island, Kanada, Kolumbien, Liechtenstein, Mazedonien, Republik Moldau, Monaco, Montenegro, Norwegen, Serbien, Schweiz, USA, EUROJUST, Internationale Kriminalpolizeiliche Organisation (IKPO-Interpol).

Folgende Drittstaaten und -stellen können nach Kenntnis der Bundesregierung mittels SIENA über einen indirekten Anschluss kommunizieren:

Bosnien und Herzegowina, Russische Föderation, Türkei, Ukraine, Civilian European Security and Defence Policy Missions, EMCDDA, OLAF, Europäische Zentralbank, European Centre for Disease Prevention and Control, Europäische Kommission, CEPOL, FRONTEX, EU Intelligence Analysis Centre, UN Office on Drugs and Crime, World Customs Organisation.

5. Inwiefern ist eine solche Teilnahme Dritter nur nach Abschluss eines Kooperationsabkommens mit Europol gestattet, und welche Regelungen müssen darin enthalten sein?

Es können nur Drittstaaten/-stellen mit einem operativen bzw. strategischen Abkommen zur Zusammenarbeit mit Europol einen Zugang zu SIENA erhalten. Der Austausch personenbezogener Daten ist hierbei nur nach Abschluss eines operativen Abkommens möglich. Die konkrete Nutzung der Applikation SIENA ist in der Regel kein Bestandteil des Abkommens zur Zusammenarbeit. Vielmehr wird im Abkommen geregelt, dass und welche inhaltlichen Informationen ausgetauscht werden dürfen. Der Zugang zu SIENA bedingt darüber hinaus die Anbindung an ein sicheres Netzwerk. Hierfür schließt Europol ergänzende bilaterale Abkommen ab, um die hierfür notwendigen technischen Vorkehrungen zu vereinbaren.

6. Welche deutschen Behörden nehmen direkt oder indirekt an SIENA teil?

SIENA wird vom Bundeskriminalamt, von der Bundespolizei, dem Zollkriminalamt, dem Landeskriminalamt Baden-Württemberg, dem Euregionalen Polizeilichen Informations- und Cooperations-Centrum (EPICC) Heerlen, dem Gemeinsamen Zentrum (GZ) Basel sowie dem Deutsch-Österreichischen Polizeikooperationszentrum (PKZ) in Passau eingesetzt.

7. Welche Staatsschutz- oder Terrorismusbehörden welcher EU-Mitgliedstaaten verfügen nach Kenntnis der Bundesregierung über einen SIENA-Zugang?

Neben Deutschland verfügen in folgenden EU-Mitgliedstaaten die für Staatsschutz oder Terrorismusbekämpfung zuständigen Behörden über einen SIENA-Zugang:

Österreich, Bulgarien, Kroatien, Zypern, Tschechien, Dänemark, Estland, Finnland, Frankreich, Griechenland, Ungarn, Irland, Italien, Litauen, Luxemburg, Niederlande, Polen, Rumänien, Slowakei, Slowenien, Spanien, Schweden, Großbritannien.

8. Welche weiteren sicheren Informationsnetze existieren für Sicherheitsbehörden auf EU-Ebene, und auf welche Weise sind diese verschlüsselt?

Für die Planung und Sicherung jedes einzelnen „Informationsnetzes“ ist der jeweilige Betreiber selbstverantwortlich. Die Vorgaben und Auswahl von einzusetzenden Kryptogeräten sind abhängig davon, welcher Regulierung die jeweilige Organisation unterliegt.

9. Was ist der Bundesregierung über Planungen bekannt, ein eigenes SIENA-Netzwerk zu Terrorismus bzw. Terrorismusabwehr einzurichten, und worum handelt es sich dabei?

Der Bundesregierung liegen Informationen vor, nach denen innerhalb des SIENA-Netzwerkes eine Closed User Group (CUG) für den Bereich Staatsschutz eingerichtet worden ist. Diese ermöglicht bi-und multilaterale Kommunikation der Staatsschutzdienststellen über SIENA.

10. Inwiefern sollen an einem solchen Netzwerk auch Dritte teilnehmen, und welche wurden hierzu nach Kenntnis der Bundesregierung angefragt?

Nach Kenntnis der Bundesregierung wurden neben den EU-Mitgliedstaaten auch die Schweiz, Island und Norwegen angefragt.

11. Welche Dokumente welcher Einstufung können derzeit unter welchen Bedingungen über SIENA kommuniziert werden?

SIENA ist derzeit bis zum Verschlussgrad „VS – Nur für den Dienstgebrauch“ akkreditiert. Höher eingestufte Dokumente dürfen nicht über SIENA ausgetauscht werden.

12. Welche Planung zum Austausch erweiterter Einstufungen existieren nach Kenntnis der Bundesregierung, und wann sollen diese umgesetzt werden?

Soweit der Bundesregierung bekannt, plant Europol eine Höherakkreditierung von SIENA auf „VS – Vertraulich“ (EU Confidential). Eine Umsetzung ist bis Ende des Jahres 2016 avisiert.

13. Inwiefern bzw. unter welcher Maßgabe wäre es aus Sicht der Bundesregierung möglich, über SIENA auch als „geheim“ eingestufte Informationen zirkulieren zu lassen?

Um über SIENA auch als „geheim“ eingestufte Informationen übertragen zu können, müsste eine sichere Übermittlung bis zum Verschlussgrad „Geheim“ gewährleistet sein. Dies ist momentan nicht der Fall.

14. Inwiefern verfügt Europol außer SIENA über weitere Kommunikationssysteme zum Austausch von als „geheim” klassifizierten Informationen, bzw. wann sollen diese eingerichtet sein?

Nach Kenntnis der Bundesregierung verfügt Europol nicht über weitere Kommunikationssysteme zum Austausch von als „Geheim“ klassifizierten Informationen. Im Übrigen wird auf die Antwort zu Frage 12 verwiesen.

15. Welche Pläne für technische oder bauliche Veränderungen bei den Agenturen Europol und Frontex sind der Bundesregierung bekannt, um zukünftig höher eingestufte Informationen und Dokumente verarbeiten zu können, und wann sind diese abgeschlossen (worden)?

Der Bundesregierung liegen hierzu keine Erkenntnisse im Sinne der Fragestellung vor. Im Übrigen wird auf die Antwort zu Frage 12 verwiesen.

16. Was ist der Bundesregierung darüber bekannt, inwiefern auch die nicht zur EU gehörende „Police Working Group on Terrorism“ (PWGT) über ein eigenes, mit SIENA vergleichbares System verfügt, und auf welche Weise ist dieses verschlüsselt?

Die Police Working Group on Terrorism (PWGT) bietet den Mitgliedstaaten unter Nutzung eines eigens dafür installierten Kryptokommunikationssystems die Möglichkeit, Informationen bis zum Verschlussgrad „Geheim“ im Bereich der Politisch motivierten Kriminalität auszutauschen. Die Verschlüsselung erfolgt hierbei hardwarebasiert und ermöglicht eine Ende-zu-Ende-Verschlüsselung zwischen den Mitgliedstaaten.

17. Inwiefern ist beabsichtigt, dass die PWGT zukünftig ebenfalls an SIENA teilnimmt?

Nach Kenntnis der Bundesregierung ist Europol bestrebt, den PWGT- Mitgliedstaaten SIENA als Kommunikationssystem anzubieten. Eine Entscheidung über die Teilnahme an SIENA obliegt den einzelnen PWGT-Mitgliedstaaten. Mit der Einrichtung einer CUG für die Staatsschutzdienststellen der EU-Mitgliedstaaten steht den hieran teilnehmenden PWGT-Mitgliedern die Nutzung von SIENA, aktuell bis zum Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“, offen.

18. Wie hat sich die Bundesregierung zu einem etwaigen entsprechenden Vorschlag verhalten?

Die Bemühungen Europols zur Höherakkreditierung von SIENA werden seitens der Bundesregierung im Grundsatz begrüßt. Innerhalb des PWGT-Verbundes bedarf es jedoch der Möglichkeit zur Übermittlung bis zum Verschlussgrad „Geheim“.

19. Auf welche Weise werden nach Kenntnis der Bundesregierung EU-Verschlusssachen (European Union classified information, EUCI) verschlüsselt, und wer hat dieses Verfahren entwickelt?

Die Frage ist aufgrund der fragmentierten Regulierung nicht spezifisch zu beantworten. Die Regeln und Prozesse sind jeweils unterschiedlich. Jeder Betreiber ist nach den für ihn geltenden Vorschriften verpflichtet, entsprechende Kryptoprodukte einzusetzen.

Der Europäische Rat verfügt über erprobte Prozesse, um die Qualität von, durch Organisationen des Europäischen Rates eingesetzte, Kryptogeräten sicherzustellen.

20. Von welchen Agenturen, sonstigen Einrichtungen der EU sowie Dritten wird EUCI nach Kenntnis der Bundesregierung genutzt?

Ob Organe und/oder Agenturen der EU zu eingestuften Informationen der EU Zugang haben bzw. solche erstellen und handhaben dürfen, hängt von der aktuellen Rechtslage ab.

Eine maßgebliche Bedingung ist der Beschluss bzw. Erlass von Geheimschutzregelungen. Unter den Organen der EU verfügen der Rat und die Europäische Kommission über ein solches Regelwerk, das sie bereits 2003 gegenseitig als gleichwertig anerkannt haben. Der 2011 ins Leben gerufene Europäische Auswärtige Dienst (EAD) hat sich ebenfalls ein solches Regelwerk gegeben. Geheimschutzregeln existieren ebenfalls für das Europäische Parlament, die jedoch aufgrund der spezifischen Bedürfnisse des Parlaments teilweise von denen des Rates, der Kommission oder des EAD abweichen. Der Europäische Gerichtshof (EuGH) ist augenblicklich dabei, solche Regeln zu erlassen. Die Europäische Zentralbank (EZB) befindet sich hierzu ebenfalls in der Phase erster Konsultationen.

Diese Regelwerke gelten jedoch nicht für EU-Agenturen. Ob und inwieweit diese Agenturen EUCI erstellen, handhaben und austauschen dürfen, hängt von der Existenz diesbezüglicher Bestimmungen in ihren jeweiligen Gründungsakten ab. Gründungsakte, die über solche Bestimmungen verfügen (z. B. für Europol, EUROJUST, Galileo Security Agency, FRONTEX oder EDA), legen in der Regel fest, dass die jeweilige Agentur die Regeln des Rates oder der Kommission entweder direkt anzuwenden oder analog in eigenen Geheimschutzregeln umzusetzen hat. Den Austausch von EUCI zwischen Organen und Agenturen der EU regeln darüber hinaus mehrere Verwaltungsabkommen. Grundsätzlich gilt: Nur die EU-Agenturen dürfen EUCI erstellen, handhaben und austauschen, die dies zur Erfüllung ihrer Aufgaben unabweisbar müssen.

Der Austausch von EUCI mit Drittstaaten bzw. internationalen Organisationen setzt wiederum den Abschluss von Geheimschutzabkommen (Security of Information Agreements) bzw. Geheimschutzübereinkommen (Security of Information Arrangements) voraus, die auch Art, Bedingungen und Umfang des Austausches regeln.

Selbstverständlich dürfen auch die Mitgliedstaaten der EU (sowohl in ihrer Eigenschaft als Mitglieder des Rates oder auch unabhängig davon) EUCI herstellen, handhaben und austauschen. Dabei haben sich die Mitgliedstaaten verpflichtet, die genannten Geheimschutzregelungen (insbesondere die des Rates), die ebenfalls nicht unmittelbar für die Mitgliedstaaten gelten, zu respektieren, um ein EU-weit einheitliches Schutzniveau zu erreichen.

21. Welche „Behörden“ hatten nach Kenntnis der Bundesregierung hinsichtlich des mutmaßlichen Attentäters Mehdi Nemmouche trotz laufender Ermittlungen ihre Informationen (etwa Ausschreibung zur verdeckten Kontrolle im Schengener Informationssystem der zweiten Generation – SIS II – sowie zur Festnahme zwecks Auslieferung) „bereits öffentlich gemacht“, sodass auch die Bundesregierung hierzu Stellung nahm (Bundestagsdrucksache 18/6223)?

Im Rahmen der Anhörung zu einem Gesetzesentwurf in der französischen Nationalversammlung machte der französische Innenminister im Lichte der damaligen Ereignisse Angaben zur Ausschreibung der genannten Person im Schengener Informationssystem.

a) Inwiefern haben „Behörden“ nach Kenntnis der Bundesregierung mittlerweile auch Informationen zur Ausschreibung des mutmaßlichen Attentäters Ayoub El K. zur verdeckten Kontrolle im SIS II oder in anderen Polizeidatenbanken „bereits öffentlich gemacht“, und zu welchen weiteren Erläuterungen sieht sich die Bundesregierung nun bereit?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

b) Seit wann war Ayoub El K. nach Kenntnis der Bundesregierung zur verdeckten Kontrolle im SIS II ausgeschrieben?

Auf die Antwort der Bundesregierung auf die Schriftliche Frage 11 des Abgeordneten Andrej Hunko vom 3. September 2015 (Bundestagsdrucksache 18/5913) wird verwiesen.

c) Auf welche Weise werden „die Länder Frankreich, Schweiz, Belgien, Deutschland und Italien“ nach Kenntnis der Bundesregierung „wo notwendig“ Passagier- und Gepäckkontrollen bei Zugreisenden intensivieren?

d) Wann und wo sollen diese Kontrollen beginnen bzw. haben sie bereits begonnen?

Die Fragen 21c und 21d werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

Auf die Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/6342 („Pläne der Verkehrs- und Innenminister der Europäischen Union zur Verschärfung der Kontrollen von Passagieren und Gepäck bei Zugreisen“) vom 14. Oktober 2015 wird verwiesen. Nach Kenntnis der Bundesregierung finden derzeit in den Stationen Paris-Nord, Bruxelles-Midi und Antwerpen-Centraal Personenkontrollen an den „Thalys-Bahnsteigen“ statt.

22. Welche Position vertritt die Bundesregierung hinsichtlich der Notwendigkeit eines EU-Systems zur Nachverfolgung der Terrorismusfinanzierung (EU-TFTP)?

Die Bundesregierung steht dem Vorschlag zur Einführung eines EU-Systems zur Nachverfolgung der Terrorismusfinanzierung offen gegenüber. Abzuwarten bleibt jedoch die konkrete Ausgestaltung der hierzu auf europäischer Ebene eingebrachten Vorschläge.

a) Welche Informationen welcher Einstufungen können Polizeien, Zoll und Geheimdienste der EU-Mitgliedstaaten derzeit mit den USA im Rahmen des SWIFT-Abkommens (SWIFT – Abkommen zwischen der Europäischen Union und den USA über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die USA für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus) austauschen?

Im Rahmen des Abkommens besteht kein direkter Kontakt zwischen deutschen Behörden und den USA. Erkenntnisse werden ausschließlich über Europol auf einem gesicherten Kanal ausgetauscht. Die Informationen sind dabei in der Regel als „VS – Nur für den Dienstgebrauch“ eingestuft. Höher eingestufte Informationen können auf dem gesicherten Kanal nicht mit Europol ausgetauscht werden.

b) Wie hat sich die Zahl von Anfragen deutscher Behörden im Rahmen des SWIFT-Abkommens sowie unaufgeforderter Meldungen (z. B. gefundene Übereinstimmungen) seitens der US-Behörden seit Einrichtung des Systems entwickelt?

Die Zahl der gemäß Artikel 10 des Abkommens gestellten Anfragen deutscher Behörden an Europol ist rückläufig. Die gemäß Artikel 9 des Abkommens seitens der US-Behörden zum Zwecke der Terrorismusbekämpfung zur Verfügung gestellten Erkenntnisse werden zahlenmäßig nicht statistisch erfasst. Sie bewegen sich jedoch nach Kenntnis der Bundesregierung auf konstantem Niveau.

c) Inwiefern werden nach Kenntnis der Bundesregierung auch nicht über SWIFT abgewickelte SEPA-Überweisungen von US-Behörden verarbeitet?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor. Daten aus dem SEPA-Zahlverfahren sind nicht Bestandteil des Abkommens zwischen der Europäischen Union und den USA über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung von der EU an die USA für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus.

d) Wie positioniert sich die Bundesregierung auf EU-Ebene zur Notwendigkeit eines zentralen Bankkontenregisters?

Deutschland besitzt mit dem Kontenabrufverfahren nach § 24 c des Gesetzes über das Kreditwesen (KWG) bereits ein solches Instrument, welches sich als Ermittlungsinstrument bewährt hat. Die Bundesregierung unterstützt daher den Vorschlag der Einführung zentraler Bankkontenregister auf EU-Ebene.

23. Auf welchen Abkommen beruht der Austausch eingestufter Informationen unter den Agenturen FRONTEX und Europol sowie dem Europäischen Auswärtigen Dienst?

Der Austausch eingestufter Informationen zwischen Europol und dem EAD erfolgt auf Basis eines bilateralen Verwaltungsabkommens. Das entsprechende Verwaltungsabkommen ist am 19. Januar 2015 in Kraft getreten.

Zwischen dem EAD und FRONTEX ist noch kein entsprechendes Verwaltungsabkommen in Kraft. Vorbereitende Gespräche zwischen den Sicherheitsbüros beider Einrichtungen haben jedoch bereits stattgefunden und der EAD hat die zeitnahe Vorlage eines ersten Entwurfs eines Verwaltungsabkommens angekündigt.

Seit dem 4. Dezember 2015 existiert ein operatives Abkommen zur Zusammenarbeit zwischen Europol und FRONTEX. Im Übrigen wird auf die Antwort zu Frage 5 verwiesen.

24. Über welche Kanäle tauschen nach Kenntnis der Bundesregierung die geheimdienstlichen EU-Lagezentren INTCEN und EUMS-INT sowie das Satellitenzentrum SatCen eingestufte Informationen mit den Agenturen FRONTEX und Europol sowie dem Europäischen Auswärtigen Dienst, und auf welchen Abkommen beruht diese Praxis?

Der Bundesregierung liegen hierzu keine Informationen vor.

25. Welche Netzwerke werden von den Agenturen FRONTEX und Europol sowie dem Europäischen Auswärtigen Dienst genutzt, um nicht eingestufte Informationen auszutauschen, und auf welche Weise werden diese verschlüsselt?

Der Bundesregierung ist im Einzelnen nicht bekannt, welche Netzwerke und Verschlüsselungssysteme die EU-Agenturen FRONTEX und Europol sowie der EAD zum Austausch nicht eingestufter Informationen nutzen.

26. Was ist der Bundesregierung über Pläne des Europäischen Auswärtigen Dienstes bekannt, zukünftig auch eingestufte Informationen mit der Europäischen Gendarmerietruppe EUROGENDFOR auszutauschen?

Derzeit erfolgt der Austausch von EUCI zwischen dem EAD und der Europäischen Gendarmerietruppe EUROGENDFOR auf Basis eines vorläufigen Geheimschutzverwaltungsabkommens zwischen dem EAD und der italienischen nationalen Sicherheitsbehörde, das am 23. Dezember 2014 in Kraft getreten ist.

Bis zum Inkrafttreten eines genuinen Geheimschutzabkommens zwischen dem EAD und der EUROGENDFOR agiert die italienische nationale Sicherheitsbehörde, nach entsprechender Einigung unter den nationalen Sicherheitsbehörden der EUROGENDFOR-Mitgliedstaaten (Italien, Frankreich, Niederlande, Portugal, Spanien und Rumänien), als „Sponsor“ der EUROGENDFOR und garantiert gegenüber dem EAD den ordnungsgemäßen Gebrauch und Schutz der ausgetauschten EUCI.

Parallel dazu hat der EAD einen Entwurf für ein genuines Geheimschutzabkommen mit EUROGENDFOR vorgelegt, der derzeit beraten wird. Es wird jedoch erst geschlossen und in Kraft treten können, wenn das EUROGENDFOR-interne Geheimschutzabkommen in Kraft getreten ist. Dazu fehlt derzeit noch die Ratifizierung dieses Abkommens durch Rumänien als jüngstem EUROGENDFOR-Mitglied. Rumänien hat die Ratifizierung für das Frühjahr 2016 in Aussicht gestellt.

a) Um welche Einstufungen handelt es sich dabei, und über welche Kanäle werden diese dann versandt?

Das in Frage 26 genannte vorläufige Geheimschutzverwaltungsabkommen sieht keine Beschränkung des VS-Grades vor und ermöglicht somit grundsätzlich – und bei Erfüllung des Grundsatzes „Kenntnis nur wenn nötig“ – den Austausch bis zum Grad TRES SECRET UE/EU TOP SECRET.

Der Austausch erfolgt grundsätzlich über die jeweiligen VS-Registraturen der beteiligten Partner.

b) Aus welchen Gründen hält die Bundesregierung den Austausch eingestufter Informationen mit der Europäischen Gendarmerietruppe für notwendig oder entbehrlich?

Die Bundesregierung hält den Austausch eingestufter Informationen mit der EUROGENDFOR für notwendig. Die Umsetzung des am 6. Oktober 2014 in Kraft getretenen generellen Verwaltungsabkommens zwischen dem EAD und der EUROGENDFOR über die Zusammenarbeit auf dem Gebiet der Gemeinsamen Verteidigungs- und Sicherheitspolitik würde ohne den Austausch von vertraulichen Informationen sehr erschwert.

27. Über welche Netzwerke werden eingestufte oder nicht eingestufte Informationen der militärischen Missionen sowie der Krisenreaktionsstrukturen und Lagezentren der EU gewöhnlich verteilt, und auf welche Weise werden diese verschlüsselt?

Informationen der militärischen Missionen werden über die Missionsnetzwerke der EU verteilt. Bei EUNAVFOR MED handelt es sich um das eingestufte Hauptinformationssystem „Mediterranean Classified Mission Network“ (MCMN). In diesem für die Führung durch das Operational Headquarter (OHQ) in Rom und vor allem für den Informationsaustausch innerhalb des Einsatzverbandes genutzten Netzwerk werden Daten bis zur Einstufung CONFIDENTIAL verarbeitet.

Für rein nationale Zwecke werden das Führungsinformationssystem Streitkräfte (FüInfoSysSK) und das Joint Analysis System Military Intelligence (JASMIN) eingesetzt.

Zur sicheren Übermittlung von Informationen im Bereich der Terrorismusbekämpfung innerhalb der europäischen Staaten wird das „Bureau de Liaison-(BdL-)-Netzwerk“ zwischen den nationalen Kontaktstellen genutzt. Weiterer Informationsaustausch wird über Standard-E-Mail oder spezifische Verschlüsselungssoftware gewährleistet.

28. Auf welche Weise bzw. über welche Netzwerke tauschen die Angehörigen der EU-Militärmission EUNAVFOR MED und der FRONTEX-Mission nach Kenntnis der Bundesregierung eingestufte oder nicht eingestufte Informationen, und auf welche Weise werden diese verschlüsselt?

EUNAVFOR MED tauscht nur mittelbar, etwa über die EU Regional Task Force (EU RTF) in Catania, mit FRONTEX Informationen aus. Auf die Antwort der Bundesregierung zu Frage 19 der Kleinen Anfrage vom 30. Oktober 2015, (Bundestagsdrucksache 18/6544) wird verwiesen.

29. Welche der beschriebenen Kryptographieverfahren auf EU-Ebene wurden von deutschen Behörden entwickelt oder umgesetzt, bzw. welche zukünftigen Pläne existieren hierfür?

Auf EU-Ebene plant der Europäische Rat mit den Mitgliedstaaten das Vorgehen bei der Entwicklung und Zulassung von kryptographischen Verfahren. Für das System JASMIN hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Freigabeempfehlung erteilt, die die Verarbeitung und Übertragung von Informationen bis einschließlich SECRET UE/EU SECRET umfasst und bis zum 30. November 2016 gültig ist.

30. Inwiefern hält es die Bundesregierung für notwendig oder entbehrlich, den Austausch eingestufter Informationen unter den Agenturen FRONTEX und Europol sowie dem Europäischen Auswärtigen Dienst und weiteren Diensten oder auch Dritten durch neue oder erweiterte Abkommen rechtlich zu regeln?

Die Bundesregierung hält es für notwendig, vor dem Austausch eingestufter Informationen zwischen den EU-Agenturen FRONTEX und Europol sowie dem EAD und weiteren Diensten oder auch Dritten entsprechende Geheimschutzabkommen bzw. Geheimschutzverwaltungsabkommen abzuschließen, um ein beiderseitig vergleichbares Schutzniveau zu garantieren.

31. Welche Stellen der Europäischen Union sind derzeit mit der Ausarbeitung neuer Abkommen oder entsprechender Studien beauftragt oder befasst?

32. Für wen sollten diese Abkommen gelten, und welche Einstufungen beträfen diese?

Die Fragen 31 und 32 werden wegen ihres Sachzusammenhangs gemeinsam beantwortet.

Alle Institutionen der EU können gegenüber dem Rat die Notwendigkeit eines Geheimschutzabkommens anzeigen und um Aufnahme entsprechender Verhandlungen bitten. Entspricht der Rat dieser Bitte, muss er gemäß Artikel 218 des Vertrags über die Arbeitsweise der Europäischen Union ein Verhandlungsmandat beschließen. Verhandlungsführung sowie Abschluss eines solchen Abkommens (Security of Information Agreement) obliegen ebenfalls dem Rat. Auf diese Weise zustande gekommene Abkommen gelten für alle EU-Einrichtungen.

Unabhängig von und unterhalb dieser Ebene erlauben die EAD-Geheimschutzregeln (2011/C 304/05) der Hohen Repräsentantin den Abschluss von Geheimschutzverwaltungsabkommen (Security of Information Arrangements), die in der Regel in Geltung und Regelungsumfang hinter den Geheimschutzabkommen zurückbleiben. Voraussetzung für dieses Verfahren ist die Zustimmung des EAD-Sicherheitsausschusses; diesem Gremium gehören alle einschlägigen nationalen Sicherheitsbehörden der EU-Mitgliedstaaten an.

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