Deutscher Bundestag **Drucksache 17/12259**

17. Wahlperiode 31. 01. 2013

Kleine Anfrage

der Abgeordneten Andrej Hunko, Jan Korte, Annette Groth, Inge Höger, Dr. Lukrezia Jochimsen, Harald Koch, Stefan Liebich, Petra Pau, Jens Petermann, Dr. Petra Sitte, Frank Tempel, Kathrin Vogler, Halina Wawzyniak, Katrin Werner und der Fraktion DIE LINKE.

Sicherheit, Datenschutz und Überwachung von Cloud-Daten

Dokumente nur vom heimischen Rechner einzusehen, ist heutzutage kaum noch vorstellbar. Von überall – egal ob vom Smartphone, von einem Internetcafe im Urlaub oder vom Rechner auf der Arbeit – auf eigene digitale Daten zugreifen zu können, ist längst Realität. Möglich machen dies die sogenannten Public-Cloud-Anbieter. So einfach die Nutzung der Public Cloud auch scheint, gibt es immer wieder Debatten hinsichtlich Sicherheit, Datenschutz und Transparenz. Kritisiert wird, dass ihre Infrastrukturen erhebliche Sicherheitsrisiken aufweisen: Die Registrierung sei zu einfach, Datenmissbrauch und -verlust kaum vermeidbar, Schnittstellen zu unsicher, die Verschlüsselung der Daten mangelhaft, Zugriffsberechtigte bei den Anbietern nicht immer vertrauenswürdig. Überdies ist es kaum nachvollziehbar, in welchem Land sich der Server des jeweiligen Anbieterunternehmens und somit auch die Daten der Nutzerinnen und Nutzer befinden. Für Public-Cloud-Anbieter gibt es keine einheitlichen Verträge und verbindlichen Standards. Je nach Verarbeitungsort können Dritte ohne großen Aufwand Zugriff auf die Daten bekommen. Hierzu gehören Geheimdienste, Strafverfolgungs-, Grenz- oder Finanzbehörden, die auf diesem Wege Informationen einholen können. Zwei Studien machen überdies darauf aufmerksam, dass Rechtsakte der US-Regierung den Zugriff ihrer Behörden sogar auf Daten außerhalb ihres Hoheitsgebietes erlauben („US-Massenüberwachung der EU-Bürger“, futurezone.at vom 15. Januar 2013). Auch kann nicht ausgeschlossen werden, dass die nationale Gesetzgebung mancher Staaten einen Zugriff von privaten Dritten, also Unternehmen, auf die Daten zulässt.

Anstatt sich der Datenschutzproblematik bei Cloud-Diensten anzunehmen, konzentriert sich die Bundesregierung auf den Zugriff ihrer Behörden auf die Daten und die Abfrage von Cloud-Passwörtern zu Ermittlungszwecken („Regierung will Abfrage von Cloud-Passwörtern erlauben“; ZEIT ONLINE vom 24. Oktober 2012). Auf mehreren Ebenen sind das Bundeskriminalamt (BKA), das Zollkriminalamt (ZKA), die Bundespolizei und das Bundesamt für Verfassungsschutz damit befasst, Polizeien und Geheimdiensten die Herausgabe von Cloud-Daten zu erleichtern. Dabei handelt es sich einerseits um die Erörterung grundsätzlicher Fragen und Rahmenbedingungen. In Projekten, Studien und Arbeitsgruppen werden aber auch technische Fragen erörtert.

Auf nationaler Ebene betreibt das Strategie- und Forschungszentrum Telekommunikation (SFZ TK) ein Projekt unter dem Namen „CLOUD“, das sich mit Fragestellungen zu Cloud-Computing und dessen Implikationen auf die Telekommunikationsüberwachung beschäftigt (Plenarprotokoll 17/210). Im SFZ TK

sind das BKA, die Bundespolizei und das Bundesamt für Verfassungsschutz gleichsam vertreten. Weitere Tätigkeitsfelder des polizeilich-geheimdienstlichen Zentrums sind die Studien „Entwicklung der Netze“, „Next Generation Network“ und „Rufnummernmanipulation“. Alle Anstrengungen drehen sich darum, wie in neuen digitalen Kommunikationsplattformen die Telekommunikationsüberwachung umgesetzt werden kann.

Zur Beteiligung der 16 Bundesländer an den Überlegungen zur Überwachung neuer Kommunikationsplattformen dient die Kommission Grundlagen der Überwachungstechnik (KomGÜT). Die Kommission soll „Synergien durch Abstimmungen und Kooperationen auf Bund-/Länderebene“ erzeugen. Beteiligt sind das BKA, das ZKA und die Bundespolizei. Das Bundesamt für Verfassungsschutz wird bei der KomGÜT als „Gast“ geführt. Auf Ebene der Landesinnenministerien betreiben die Länderpolizeien zudem einen Unterausschuss Information und Kommunikation (UA IuK), der beim Arbeitskreis II – Innere Sicherheit der Arbeitsgemeinschaft der Innenministerien der Länder angesiedelt ist.

Um auch international Einfluss auf die Standardisierung der Telekommunikationsüberwachung von Cloud-Diensten zu nehmen, engagieren sich deutsche Polizeibehörden überdies in internationalen Netzwerken. Eine besondere Rolle kommt dem European Telecommunications Standards Institute (ETSI) zu, das einen „Technische[n] Report“ zu Cloud-Diensten erarbeitet (Bundestagsdrucksache 17/11598). Das Normungsinstitut sucht dafür die Zusammenarbeit deutscher Provider, darunter der Deutschen Telekom AG und Telefonica O2. Auch die Bundesnetzagentur wurde dafür angesprochen. Bekanntlich arbeitet die Aachener Überwachungssparte des Utimaco-Konzerns im Technischen Komittee für Telekommunikationsüberwachung (TC LI) des ETSI mit (www.tinyurl.com/cw3aq4k). Die Firma stellt Abhörschnittstellen (Lawful Interception Management Systems) her. In der Arbeitsgruppe wird der Bedarf zukünftiger Abhörtechnologie durch Ermittlungsbehörden und Geheimdienste festgelegt. Auch das Bundesamt für Verfassungsschutz und die Bundesnetzagentur sind beteiligt. Zu den international aktiven Akteuren hinsichtlich der Überwachung der Telekommunikation gehören neben dem Bundesamt für Sicherheit in der Informationstechnik (BSI) auch das Landesamt für Zentrale Polizeiliche Dienste (LZPD) der Landespolizei Nordrhein-Westfalen.

Die Fragestellerinnen und Fragesteller sehen die Anstrengungen zur Überwachung von Cloud-Diensten überaus kritisch. Die beteiligten Behörden untergraben damit das ohnehin gestörte Vertrauen in die Freiheit des Internets. Zudem wird das Trennungsgebot von Polizei und Geheimdiensten in den genannten Gremien zunehmend ausgehöhlt. Es kann deshalb nicht hingenommen werden, wenn die Fragen zu dem Gebaren und den Aktivitäten der Behörden nicht öffentlich beantwortet werden.

Wir fragen die Bundesregierung:

1. Mit welchen Gesetzgebungsinitiativen, Forschungsprojekten, Studien und Verfahren zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten sind deutsche Behörden gegenwärtig befasst?
2. Inwieweit betreibt das Bundeskriminalamt eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?
   a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?
   b) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet das BKA hierfür zusammen?

c) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

d) Inwieweit sind diese öffentlich zugänglich?

3. Inwieweit betreibt das Zollkriminalamt eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet das ZKA hierfür zusammen?

c) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

d) Inwieweit sind diese öffentlich zugänglich?

4. Inwieweit betreibt die Bundespolizei eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet die Bundespolizei hierfür zusammen?

c) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

d) Inwieweit sind diese öffentlich zugänglich?

5. Inwieweit betreibt das Bundesamt für Verfassungsschutz eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet das Bundesamt für Verfassungsschutz hierfür zusammen?

c) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

d) Inwieweit sind diese öffentlich zugänglich?

6. Inwieweit betreibt die Bundesnetzagentur eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet die Bundesnetzagentur hierfür zusammen?

c) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

d) Inwieweit sind diese öffentlich zugänglich?

7. Inwieweit betreibt das Bundesamt für Sicherheit in der Informationstechnik eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet das BSI hierfür zusammen?

c) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

d) Inwieweit sind diese öffentlich zugänglich?

8. Inwieweit betreiben der Bundesnachrichtendienst (BND) und der Militärische Abschirmdienst (MAD) eigene Anstrengungen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeiten der BND und der MAD hierfür zusammen?

c) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

d) Inwieweit sind diese öffentlich zugänglich?

9. Welche Überlegungen führten dazu, das in der Vergangenheit beim Bundesverwaltungsamt angesiedelte Kompetenzzentrum der Zentralstelle für Telekommunikationstechnologien in das Strategie- und Forschungszentrum Telekommunikation zu überführen?

a) Welche Aufgaben hatte das frühere Kompetenzzentrum der Zentralstelle für Telekommunikationstechnologien, und wer war daran beteiligt?

b) Inwiefern unterscheiden sich die Aufgaben des SFZ TK vom früheren Kompetenzzentrum der Zentralstelle für Telekommunikationstechnologien?

c) Wo ist das SFZ TK angesiedelt?

d) Über welchen Haushalt verfügt das SFZ TK, und wie wird es finanziert?

e) Inwiefern wurde bei der Einrichtung des SFZ TK erörtert, ob dadurch das Trennungsgebot von Geheimdiensten und Polizei aufgeweicht werden könnte?

10. Welche weiteren Details kann die Bundesregierung zum Projekt „CLOUD“ mitteilen, das sich mit Fragestellungen zu Cloud-Computing und dessen Implikationen auf die Telekommunikationsüberwachung beschäftigt (Plenarprotokoll 17/210)?

a) Unter wessen Leitung steht das Projekt „CLOUD“?

b) Wer hat die Einrichtung des Projekts angeregt und verfügt?

c) Welche Arbeitsgruppen oder Unterarbeitsgruppen existieren im Projekt?

d) Welche konkreten Aufgaben übernehmen das BKA, die Bundespolizei und das Bundesamt für Verfassungsschutz im Rahmen des Projekts?

e) Welche Treffen haben hierzu stattgefunden, und wer nahm daran teil?

f) Welche weiteren Institutionen, Firmen oder wissenschaftlichen Einrichtungen wurden für das Projekt mit welchem Ziel angesprochen?

g) Wie haben die Angesprochenen darauf reagiert?

h) Welche weiteren Institutionen, Firmen oder wissenschaftlichen Einrichtungen sollen zukünftig für das Projekt angesprochen werden?

i) Wann, wo und wem werden etwaige Ergebnisse des Projekts „CLOUD“ vorgestellt und beraten?

j) Inwieweit sind diese öffentlich zugänglich?

11. Auf welche Art und Weise bzw. mit welchem Inhalt wurden innerhalb von „CLOUD“ folgende Themen erörtert oder bearbeitet:

a) Software und Betriebssysteme,

b) auf verschlüsselten Kommunikationsprotokollen basierender Zugang zu Cloud-Diensten,

c) Zugriff der Sicherheitsbehörden,

d) Forensik?

12. Welche weiteren Details kann die Bundesregierung zu Inhalten, Zielsetzung und Beteiligten der Studien „Entwicklung der Netze“, „Next Generation Network“ und „Rufnummernmanipulation“ mitteilen (Plenarprotokoll 17/210)?

13. Auf welche Weise befasst sich die Kommission Grundlagen der Überwachungstechnik mit der (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Welche „Synergien durch Abstimmungen und Kooperationen auf Bund-/Länderebene“ wurden hinsichtlich der (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten bereits erzeugt bzw. welche sind angestrebt?

b) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

c) Unter wessen Leitung stehen die Vorhaben?

d) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet die KomGÜT hierfür zusammen?

e) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

f) Inwieweit sind diese öffentlich zugänglich?

g) Inwiefern wurde innerhalb der KomGÜT erörtert, ob durch die Mitarbeit des Bundesamtes für Verfassungsschutz (auch als „Gast“) das Trennungsgebot von Geheimdiensten und Polizei aufgeweicht werden könnte?

14. Auf welche Weise befasst sich der Unterausschuss Information und Kommunikation nach Kenntnis der Bundesregierung mit der (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?

a) Auf wessen Initiative kamen die Vorhaben zustande, und wie werden diese finanziert?

b) Unter wessen Leitung stehen die Vorhaben?

c) Mit welchen weiteren Behörden, Firmen oder anderen Institutionen arbeitet die KomGÜT hierfür zusammen?

d) Wann und wo werden etwaige Ergebnisse der Vorhaben vorgestellt und beraten?

e) Inwieweit sind diese öffentlich zugänglich?

15. Auf welche Weise befassen sich Agenturen oder Ratsarbeitsgruppen der Europäischen Union mit konkreten Vorhaben der (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten bzw. deren gesetzlichen und organisatorischen Rahmenbedingungen?
16. Welche weiteren Details kann die Bundesregierung zum „Technische[n] Report“ zu Cloud-Diensten des European Telecommunications Standards Institute mitteilen (Bundestagsdrucksache 17/11598)?
    a) Unter wessen Leitung steht der „Technische Report“?
    b) Wer hat die Einrichtung des Projekts angeregt und verfügt?
    c) Welche konkreten Aufgaben übernehmen das BKA, die Bundespolizei und das Bundesamt für Verfassungsschutz im Rahmen des Projekts?
    d) Welche Treffen haben hierzu stattgefunden, und wer nahm daran teil?
    e) Welche weiteren Institutionen, Firmen oder wissenschaftlichen Einrichtungen wurden für das Projekt mit welchem Ziel angesprochen?
    f) Wie haben die Angesprochenen darauf reagiert?
    g) Welche weiteren Institutionen, Firmen oder wissenschaftlichen Einrichtungen sollen zukünftig für das Projekt angesprochen werden?
    h) Wann und wo wird der „Technische Report“ vorgestellt und beraten?
    i) Inwieweit ist dieser öffentlich zugänglich?
17. Welche Treffen der Arbeitsgruppen TC LI und SA 3 LI des ETSI haben nach Kenntnis der Bundesregierung bzw. ihrer teilnehmenden Behörden in den letzten fünf Jahren an welchen Orten in Deutschland stattgefunden?
    a) Welche deutschen Firmen oder Behörden waren für die Einladung oder Tagesordnung jeweils verantwortlich?
    b) Welche deutschen Firmen oder Behörden haben an den Treffen teilgenommen?
    c) Welche Teilnehmer/-innen sind ihren Behörden noch erinnerlich, sofern die Bundesregierung über keine Teilnahmelisten verfügt?
    d) Mit welchen Zielen und mit welchen Initiativen haben sich das Landesamt für Zentrale Polizeiliche Dienste der Polizei Nordrhein-Westfalen und (soweit den Beteiligten der Bundesregierung bekannt oder erinnerlich) der Aachener Hersteller von Überwachungstechnologien Utimaco in den letzten fünf Jahren in den Arbeitsgruppen TC LI und SA 3 LI eingebracht?
18. Auf welche Weise befasst sich die Internationale Fernmeldeunion (ITU) nach Kenntnis der Bundesregierung mit der (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten?
    a) Inwiefern wurde die Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten auch auf der World Conference on International Telecommunications (WCIT) in Dubai thematisiert?
    b) Wie hat sich die Bundesregierung zu entsprechenden Dokumenten oder Abstimmungen verhalten?
19. Wie beurteilt die Bundesregierung das Ergebnis der im Auftrag des Ausschusses für Bürgerrecht, Justiz und Inneres des EU-Parlaments in Auftrag gegebenen Studie des Centre D’Etudes sur les Conflits und des Centre for European Policy Studies, wonach die größte Gefahr beim Cloud-Computing nicht in der Cyberkriminalität, sondern durch Zugriffe von Behörden bestünde („Fighting cyber crime and protecting privacy in the cloud“, European Parliament 2012)?

20. Welche Rechtsakte der US-Regierung sind der Bundesregierung bekannt, die einen Zugriff durch US-Behörden auf in den USA befindlichen Cloud-Servern gespeicherte Daten von Nutzerinnen und Nutzern aus der Europäischen Union ermöglichen?

    a) Inwieweit wurde die Bundesregierung von welchen Stellen der US-Regierung hierüber in Kenntnis gesetzt, etwa im Rahmen der kürzlichen Verlängerung des sogenannten Foreign Intelligence Surveillance Act (FISA) durch den US-Präsidenten Barack Obama oder des sogenannten Patriot Act?

    b) Inwiefern hat die Bundesregierung sichergestellt, dass betroffene deutsche Staatsangehörige von etwaigen Abhörmaßnahmen im Vorfeld oder nachträglich unterrichtet werden?

    c) Inwiefern ist für die Durchsuchung der Cloud-Daten nach den jeweiligen Rechtsakten eine richterliche Genehmigung erforderlich?

21. Inwiefern ist der Bundesregierung bekannt, ob der Patriot Act oder der FISA auch Zugriffe von US-Behörden außerhalb der USA erlaubt, wie es niederländische Wissenschaftler kürzlich in einer Studie beschrieben hatten („Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act“, November 2012)?

    a) Wenn ja, wie bewertet die Bundesregierung die Rechtmäßigkeit eines Zugriffs von US-Behörden auf in Deutschland gespeicherte oder prozessierte Daten bei Unternehmen, Behörden oder sonstigen Stellen?

    b) Inwieweit ist diese Praxis durch Rechtshilfeabkommen der Bundesregierung mit den USA gedeckt, bzw. inwieweit widerspricht sie diesen?

    c) Inwieweit treffen Medienberichte zu, wonach weder der EU-Kommission noch dem EU-Parlament oder nationalen Datenschützern die Möglichkeit des US-Zugriffs auf Daten im Ausland bekannt war (Die Presse, 11. Januar 2013)?

    d) Inwiefern sieht sich die Bundesregierung auch durch Medienberichte veranlasst, die Auslegung des Patriot Act oder des FISA für Spionagemaßnahmen auf ihrem Hoheitsgebiet zu unterbinden, und welche Schritte hat sie gegenüber welchen US-Stellen bereits unternommen?

    e) Wie werden die Bundesregierung und die EU zukünftig dafür sorgen, dass Cloud-Daten in Deutschland bzw. in der EU vor Abfragen aus den USA geschützt werden (bitte die konkreten Maßnahmen, Rechtsakte oder sonstigen Schritte erläutern)?

22. Wie viele Rechtshilfeersuchen zur Sicherung oder Herausgabe von Cloud-Daten haben welche Bundesbehörden in den letzten zwei Jahren bei welchen Einrichtungen welcher Länder gestellt?

    a) Wie viele Rechtshilfeersuchen zur Sicherung oder Herausgabe von Cloud-Daten haben welche Behörden welcher Länder in den letzten zwei Jahren bei welchen Bundesbehörden gestellt?

    b) Wie wurden die Rechtshilfeersuchen jeweils beantwortet?

    c) Welche sonstigen Angaben kann die Bundesregierung zu deren Umfang und Beantwortung machen, sofern sie die Rechtshilfeersuchen und ihren Ausgang nicht protokolliert?

23. Trifft es zu, dass die Bundesregierung die Abfrage von Cloud-Passwörtern im Rahmen des neuen Telekommunikationsgesetzes erleichtern möchte?

    a) Wie würde dieser Grundrechtseingriff begründet?

    b) Inwiefern wäre hierfür ein Richtervorbehalt notwendig?

24. Wie steht die Bundesregierung zu den Ausführungen des Strafrechtlers und Juniorprofessors Dr. Tobias Singelnstein, wonach sich technische Möglichkeiten zum Knacken der Passwörter von Cloud-Diensten für die Strafverfolgung verbieten, da diese nicht von der Strafprozessordnung gedeckt sind (NStZ – Neue Zeitschrift für Strafrecht, Heft 11/2012, S. 593 bis 606)?

    a) Auf welcher rechtlichen Grundlage hält die Bundesregierung das heimliche Auslesen von Mobiltelefonen, etwa im Polizeigewahrsam oder bei Grenzkontrollen, für zulässig?

    b) Inwiefern ist hierfür ein richterlicher Beschluss vonnöten?

    c) In welchem Umfang wird dies von welchen Bundesbehörden praktiziert?

    d) Auf welcher rechtlichen Grundlage hält die Bundesregierung die Einrichtung von Schnittstellen zum unbemerkten Ausleiten des Datenverkehrs bei Telekommunikationsanbietern für unbedenklich?

25. Über welche technischen Werkzeuge (Hardware, Software) verfügen welche Bundesbehörden zum Auslesen, Erraten oder Knacken von Passwörtern von Internetdiensten oder Kommunikationsgeräten?

26. Inwiefern wurden nach Kenntnis der Bundesregierung in die genannten Vorhaben und Initiativen zur (zukünftigen) Überwachung, Sicherung und Herausgabe von Daten bei Cloud-Diensten auch Vertreter/-innen aus den Bereichen Datenschutz, Bürgerrechte oder Netzpolitik eingebunden (insbesondere im SFZ TK, in der KomGÜT, dem UA IuK und dem ETSI)?

Berlin, den 31. Januar 2013

Dr. Gregor Gysi und Fraktion

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, 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