Deutscher Bundestag **Drucksache 19/17218**

19. Wahlperiode 17.02.2020

Vorabfassung - wird durch die lektorierte Version ersetzt.

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Maria Klein-Schmeink, Dr. Konstantin von Notz, Dr. Bettina Hoffmann, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 19/16949 –

Schwachstellen bei der Ausgabe von elektronischen Ausweisen und Komponenten der Telematikinfrastruktur im Gesundheitswesen

Vorbemerkung der Fragesteller

Mitglieder des Chaos Computer Clubs (CCC) haben am 27. Dezember 2019 beim 36. Chaos Communication Congress in Leipzig Schwachstellen und Sicherheitslücken beim Ausgabeprozess für verschiedene in der Telematikinfrastruktur (TI) genutzte Komponenten und Smartcards demonstriert. Sie konnten zeigen, wie es für Unbefugte problemlos möglich war, einzelne Smartcards und Komponenten der TI durch die jeweiligen beteiligten Serviceprovider zu beziehen (https://e-health-com.de/details-news/ccc-hackt-bestellprozess-gematik-nimmt-stellung/). Es gelang den CCC-Mitgliedern, sich u. a. unautorisiert einen elektronischen Heilberufeausweis und einen Praxisausweis (SMC-B) zu bestellen. Auch ein Konnektor wurde den CCC-Mitgliedern unautorisiert ausgehändigt. Zusätzlich waren bei einem beauftragten Serviceprovider die Kartenanträge von 168 Ärztinnen und Ärzten zeitweise online zugänglich.

Außerdem war es den Mitgliedern des CCC gelungen, unautorisiert eine elektronische Gesundheitskarte der AOK Hessen zu bestellen (https://e-health-com.de/details-news/ccc-hackt-bestellprozess-gematik-nimmt-stellung/). Vor dem Hintergrund, dass bereits 2015 Recherchen des ZDF Schwachstellen bei der Ausgabe der elektronischen Gesundheitskarte offengelegt haben (vgl. Deutsche Apothekerzeitung vom 25. Juni 2015 „Massives Sicherheitsleck bei Gesundheitsdaten“, abrufbar unter https://www.deutsche-apotheker-zeitung.de/news/artikel/2015/06/25/unnamed-75), stellt sich die Frage, warum es noch immer zu derartigen Problemen bei der Ausgabe von elektronischen Ausweisen und Komponenten der Telematikinfrastruktur kommt, die auch im Stande sind, die Akzeptanz der Digitalisierung des Gesundheitswesens zu gefährden.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Gesundheit vom 13. Februar 2020 übermittelt.

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

Vorabfassung - wird durch die lektorierte Version ersetzt.

Vorbemerkung der Bundesregierung

Mitglieder des Chaos Computer Clubs haben Schwachstellen in den Ausgabeprozessen für Heilberufsausweis, Praxisausweis und elektronische Gesundheitskarte bei den Kartenherausgebern identifiziert. Zu keinem Zeitpunkt waren dabei medizinische Daten gefährdet. Die Gesellschaft für Telematik und die zuständigen Aufsichtsbehörden haben schnell und entschlossen reagiert und die Ausgabe der Arzt- und Praxisausweise temporär gestoppt. Nach Behebung der Schwachstellen konnten die Ausgabeprozesse in der Zwischenzeit wieder aufgenommen werden.

Datenschutz und Datensicherheit haben für die Bundesregierung beim Aufbau der Telematikinfrastruktur oberste Priorität. Deshalb sind Schwachstellen, wie sie der Chaos Computer Club aufgedeckt hat, nicht akzeptabel.

Der Aufbau der Telematikinfrastruktur befindet sich immer noch in einer recht frühen Phase. Noch werden keine medizinischen Behandlungsdaten gespeichert. Deshalb begrüßt die Bundesregierung ausdrücklich, dass die Schwachstellen entdeckt und behoben wurden.

1. Wie bewertet die Bundesregierung die durch Mitglieder des CCC offenbarten Schwachstellen und Sicherheitslücken beim Ausgabeprozess für verschiedene in der Telematikinfrastruktur genutzte Komponenten und Smartcards (vgl. https://www.ccc.de/en/updates/2019/neue-schwachstellen-gesundheitsnetzwerk), und teilt die Bundesregierung die Ansicht der Fragesteller, dass diese, sollten sie nicht schnellstmöglich abgestellt werden, im Stande sind, die Akzeptanz der Digitalisierung des Gesundheitswesens zu gefährden?

Mitglieder des Chaos Computer Clubs haben Schwachstellen in den Ausgabeprozessen für Heilberufsausweis, Praxisausweis und elektronischer Gesundheitskarte bei den Kartenherausgebern identifiziert. Zu keinem Zeitpunkt waren dabei medizinische Daten gefährdet. Die Gesellschaft für Telematik und die zuständigen Aufsichtsbehörden haben schnell und entschlossen reagiert und die Ausgabe der Arzt- und Praxisausweise temporär gestoppt. Nach Behebung der Schwachstellen konnten die Ausgabeprozesse in der Zwischenzeit wieder aufgenommen werden.

2. Welche konkreten Maßnahmen ergreift die Bundesregierung in Kooperation mit den jeweils zuständigen Stellen vor dem Hintergrund der Recherchen von Mitgliedern des Chaos Computer Clubs im Hinblick

   a) auf den Prozess der Ausgabe der elektronischen Gesundheitskarte,

Die Ausgabeprozesse der elektronischen Gesundheitskarte unterliegen seit dem 6. Februar 2020 der Richtlinie nach § 217f des Fünften Buches Sozialgesetzbuch (SGB V). Gleichzeitig sieht der Referentenentwurf des Patientendaten-Schutzgesetzes die Übertragung einer zentralen Rolle bei der sicheren Ausgestaltung der Ausgabeprozesse für elektronische Gesundheitskarten an die Gesellschaft für Telematik und die Verschärfung der Anforderungen an die Richtlinie nach § 217f SGB V vor.

   b) auf den Prozess der Ausgabe von eHBA und SMC-B,

Die Gesellschaft für Telematik und die zuständigen Aufsichtsbehörden haben schnell und entschlossen reagiert und die Ausgabe der Arzt- und Praxisausweise temporär gestoppt. Nach Behebung der Schwachstellen konnten die Ausgabeprozesse in der Zwischenzeit wieder aufgenommen werden. Gleichzeitig

plant das Bundesministerium für Gesundheit im Rahmen des Patientendaten-Schutzgesetzes der Gesellschaft für Telematik auch für die Ausgabe von SMC-B (Institutionskarte) und Heilsberufsausweisen (HBA) eine zentrale Rolle zur sicheren Ausgestaltung der Ausgabeprozesse zu übertragen.

c) auf den Prozess der Ausgabe von Komponenten wie Konnektoren und Kartenterminals?

Es wird auf die Antwort zu Frage 5 verwiesen.

3. Wie häufig ist es nach Kenntnis der Bundesregierung Unbefugten bislang gelungen, unautorisiert an bestimmte Karten und Komponenten zu gelangen (bitte detailliert jeweils nach Herausgeber für eGK, eHBA, SMC-B, HSM-B, ggf. gSMC-KT, Kartenterminals und Konnektoren darstellen)?

   Wenn die Bundesregierung hierzu noch keine Kenntnisse hat, wann wird sie dem Deutschen Bundestag hierzu einen detaillierten Bericht vorlegen?

Die Untersuchungen für die Heilsberufsausweise (eHBA) sind abgeschlossen. Es wurden nur die beiden aus den Medien bekannten und zu Demonstrationszwecken durchgeführten Fälle identifiziert, bei denen jeweils der Karteninhaber sein Einverständnis gab. Die Untersuchungen für den Kartentyp SMC-B durch die Gesellschaft für Telematik dauern noch an. In Bezug auf die elektronische Gesundheitskarte (eGK) liegen der Bundesregierung keine Erkenntnisse vor. Ein Produkt vom Produkttyp HSM-B wurde noch nicht zugelassen, sodass der Auslieferungsprozess auch nicht betroffen ist. Zum Auslieferungsprozess von Kartenterminal (einschließlich gSMC-KT) und Konnektor wird auf die Antwort zu Frage 5 verwiesen.

4. Wie war zum Zeitpunkt der Recherchen des CCC nach Kenntnis der Bundesregierung der konkrete Ablauf des Kartenherausgabeprozesses für die in der Telematik genutzten Smartcards (bitte detailliert jeweils für eGK, eHBA, SMC-B, HSM-B, ggf. gSMC-KT und getrennt nach den jeweiligen Herausgebern der Karten wie Kassen, Kammern, KVen und KZVen darstellen)?

7. Wurde nach Kenntnis der Bundesregierung der Ausgabeprozess für die jeweiligen Karten (eGK, eHBA, SMC-B, HSM-B, ggf. gSMC-KT) spezifiziert (bitte für jede Karte darstellen)?

   Wenn ja, wann, und durch wen?

   Wenn nein, warum nicht, und beabsichtigt die Bundesregierung für die Zukunft eine solche Spezifizierung vorzugeben?

8. Wurde der jeweilige Ausgabeprozess für die jeweiligen Karten zugelassen?

   Wenn ja, wann, und durch wen?

   Wenn nein, warum nicht, und beabsichtigt die Bundesregierung für die Zukunft eine solche Zulassung?

Die Fragen 4, 7 und 8 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Ausgabeprozesse der eGK, des HBA und der SMC-B werden zurzeit durch die jeweiligen Kartenherausgeber verantwortet und unterliegen deren Zulassungsbestimmungen. Dementsprechend kann diese Frage nicht zentral beant-

Vorabfassung - wird durch die lektorierte Version ersetzt.

wortet werden. Zukünftig wird die Identifizierung des Antragstellers innerhalb des Antrags-, Herausgabe- und Freischaltungsprozesses jedoch durch die Gesellschaft für Telematik festgelegt, direkt bei den Anbietern umgesetzt und durch die Gesellschaft für Telematik geprüft. Die Identifizierung des Antragstellers liegt dann nicht mehr in der Verantwortung der Sektoren.

Gleichzeitig plant das Bundesministerium für Gesundheit im Rahmen des Patientendaten-Schutzgesetzes der Gesellschaft für Telematik eine zentrale Rolle zur sicheren Ausgestaltung der Ausgabeprozesse zu übertragen. In Bezug auf HSM-B und Gerätekarte des Kartenterminals (gSMC-KT) wird auf die Antworten zu den Fragen 3 und 5 verwiesen.

5. Wie war zum Zeitpunkt der Recherchen des CCC nach Kenntnis der Bundesregierung der konkrete Ablauf des Herausgabeprozesses für die in der Telematik benutzten Komponenten Konnektor und Kartenterminal?

Kartenterminal und Konnektor unterliegen einer sicheren Lieferkette. Die sichere Lieferkette dient zur Vermeidung von Manipulationen während der Auslieferung und ggf. einer Zwischenlagerung. Wie dieser Lieferprozess ausgestaltet ist, ist herstellerspezifisch und in den Handbüchern der Hersteller beschrieben.

Die gSMC-KT wird mit dem Kartenterminal ausgeliefert. Sie ist nicht spezifisch auf die Verwenderin bzw. den Verwender personalisiert. Insofern ist in diesem Fall kein Beantragungsprozess notwendig. Kartenterminal und Konnektor sind prinzipiell von jedermann bestellbar. Der reine Besitz dieser Geräte berechtigt nicht zum Zugang zur Telematikinfrastruktur.

6. Wurden nach Kenntnis der Bundesregierung alle Herausgabeprozesse sowohl für Smartcards als auch für Komponenten im Hinblick auf die zuverlässige und eindeutige Identifizierung der Empfänger von Karten und Komponenten überprüft?

   Wenn ja, wann, durch wen, und mit welchem Ergebnis?

   Wenn nein, warum nicht?

Die Ausgabeprozesse für die Ausgabe der Arzt- und Praxisausweise wurden temporär gestoppt. Nach Behebung der Schwachstellen konnten die Ausgabeprozesse in der Zwischenzeit wieder aufgenommen werden.

Zum Ausgabeprozess der Komponenten und der gSMC-KT wird auf die Antwort zu den 4 und 5 verwiesen.

9. a) Welche Verfahren zur sicheren und eindeutigen Identifizierung der Empfängerinnen und Empfänger von Karten und Komponenten gibt es nach Kenntnis der Bundesregierung, und warum wurden diese nicht von vornherein verbindlich als einzig mögliche Verfahren vorgegeben?

Es wird auf die Antwort zu den Fragen 4, 7 und 8 verwiesen.

Vorabfassung - wird durch die lektorierte Version ersetzt.

b) Trifft es zu, dass die Bundesnetzagentur unsichere Verfahren wie „BankIdent“ und „KammerIdent“ inzwischen deaktiviert hat (https://e-health-com.de/details-news/ccc-hackt-bestellprozess-gematik-nimmt-stellung/), und wenn ja, warum ist dies erst nach den Berichten über die Rechercheergebnisse des CCC geschehen?

Die von akkreditierten Konformitätsbewertungsstellen überprüften und positiv bewerteten, bislang unauffälligen Verfahren wurden in Absprache mit den Anbietern am gleichen Tag bzw. am Folgetag, nach der Information durch den Chaos Computer Club, abgeschaltet, also bereits vor den Berichten über die Rechercheergebnisse auf dem Chaos Communication Congress. Ob und inwieweit es sich bei den Verfahren um konzeptuell unsichere Verfahren handelt oder ob und inwieweit mangelhafte Anwendung vorhandener Sicherheitsmaßnahmen vorliegt, ist gegenwärtig in der Prüfung.

10. Wurden die bei der Ausgabe der Karten beteiligten Serviceprovider (Medisign, Bundesdruckerei, T-Systems) nach Kenntnis der Bundesregierung jeweils zugelassen bzw. in anderer Weise überprüft?

Wenn ja, wann, und durch wen?

Wenn nein, warum nicht, und beabsichtigt die Bundesregierung für die Zukunft eine solche Zulassung oder zumindest Überprüfung vorzugeben?

Die genannten Anbieter wurden vor ihrer Zulassung entsprechend der auf der Internetseite der Gesellschaft für Telematik veröffentlichten Zulassungskriterien, einschließlich der Sicherheitsvorgaben, geprüft. Diese Vorgaben umfassten in der Vergangenheit jedoch nicht die vom Chaos Computer Club berechtigterweise beanstandeten Antrags- und Ausgabeprozesse, da diese in der Verantwortung der Kartenherausgeber lagen.

11. Ist in Bezug auf Frage 10 nach Kenntnis der Bundesregierung ein Entzug der jeweiligen Zulassung der beteiligten Serviceprovider denkbar, beispielsweise für den Fall, dass diese die bekannt gewordenen Schwachstellen und Sicherheitslücken nicht schnellstmöglich abstellen oder sich im Zuge weiterer Überprüfungen als nicht vertrauenswürdig erweisen?

Zugelassenen Anbietern kann die Zulassung wieder entzogen werden, sofern diese die Zulassungsbedingungen nicht mehr erfüllen. Wie bereits ausgeführt, waren die vom Chaos Computer Club demonstrierten Schwachstellen bisher nicht Gegenstand der Zulassungsbedingungen.

Das Bundesministerium für Gesundheit hat im Rahmen des Referentenentwurf eines Patientendaten-Schutzgesetzes weitere Bußgeldtatbestände und eine deutliche Erhöhung des Bußgeldrahmens vorgesehen.

12. Warum ist es nach Kenntnis der Bundesregierung offenbar noch immer möglich (vgl. https://e-health-com.de/details-news/ccc-hackt-bestellprozess-gematik-nimmt-stellung/), bei einzelnen Krankenkassen durch Adressänderungen ohne eine sichere Identifizierung unbefugt an eine elektronische Gesundheitskarte zu gelangen, obwohl die diesbezüglichen Schwachstellen beim Ausgabeprozess seit langem bekannt sind?

13. a) Welche Maßnahmen haben die Bundesregierung, der GKV-Spitzenverband und die Aufsichtsbehörden der Länder seit 2015 konkret ergriffen, um die Ausgabe von elektronischen Gesundheitskarten an Unbefugte zu verhindern oder zumindest zu erschweren?

Vorabfassung - wird durch die lektorierte Version ersetzt.

b) Wurde die Umsetzung dieser Maßnahmen durch die Bundesregierung bzw. die Aufsichtsbehörden der Länder überprüft, und wenn ja, wann ,und wie konkret?

Wenn nein, warum ist dies bislang unterblieben, und ist geplant, dieses schwerwiegende Versäumnis nachzuholen?

Die Fragen 12 und 13 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Der Spitzenverband Bund der Krankenkassen erhielt durch § 271f Absatz 4b SGB V den Auftrag, eine Richtlinie zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme bis zum 14. Dezember 2018 zu erstellen. Die Richtlinie wurde in Abstimmung mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und dem Bundesamt für Sicherheit in der Informationstechnik fristgemäß erstellt und den Krankenkassen mit Rundschreiben vom 6. Februar 2019 bekanntgegeben. Laut der Richtlinie sind die darin gelisteten Anforderungen innerhalb von 12 Monaten für bestehende Verfahren, also bis zum 6. Februar 2020, umzusetzen.

In der Richtlinie wird u. a. geregelt, welche Anforderungen für eine sichere Authentifizierung des Versicherten durch die Kassen erfüllt werden müssen und wie eine sichere Übermittlung von Daten auf postalischem oder elektronischem Weg zu erfolgen hat. Gleichzeitig plant das Bundesministerium für Gesundheit im Rahmen des Patientendaten-Schutzgesetzes der Gesellschaft für Telematik eine zentrale Rolle bei der sicheren Ausgestaltung der Ausgabeprozesse zu übertragen und die Anforderungen an die Richtlinie nach § 217f SGB V zu verschärfen.

14. Kann nach Kenntnis der Bundesregierung mittels eines elektronischen Heilberufeausweises (eHBA) aktuell eine qualifizierte elektronische Signatur (QES) erzeugt werden, und für welche Zwecke kann diese QES derzeit genutzt werden?

Der eHBA erlaubt die Erzeugung einer qualifizierten elektronischen Signatur (QES) nach der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014. Die QES wird zurzeit insbesondere im Rahmen von Pilotprojekten zum Beispiel zum E-Rezept und zum elektronischen Arztbrief verwendet.

15. Welche Angriffsszenarien sind nach Auffassung der Bundesregierung möglich, solange die Gefahr besteht, dass für die Telematikinfrastruktur notwendige Karten und Komponenten weiterhin an Unbefugte ausgegeben werden?

Alle vom Chaos Computer Club aufgezeigten Schwachstellen, die zu einer Ausgabe von Karten an Unbefugte hätten führen können, wurden in der Zwischenzeit adressiert.

16. Welche konkreten datenschutzrechtlichen Bestimmungen sind nach Auffassung der Bundesregierung in den vom CCC durchgeführten Fällen des unautorisierten Bezuges von Smart Cards und Komponenten der TI einschlägig, um die Verantwortlichkeit der ausgebenden Stellen zu überprüfen und ggf. zu sanktionieren?

Die Prüfung, ob im Einzelfall ein Verstoß gegen datenschutzrechtliche Vorschriften vorliegt, obliegt den zuständigen datenschutzrechtlichen Aufsichtsbe-

Vorabfassung - wird durch die lektorierte Version ersetzt.

hörden. Der Landesbeauftragte für den Datenschutz ist zuständige Aufsichtsbehörde für die öffentlichen Stellen des jeweiligen Landes, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit für die öffentlichen Stellen des Bundes. Für nicht-öffentliche Stellen ist die in dem jeweiligen Land zuständige Aufsichtsbehörde zuständig.

Die seit dem 25. Mai 2018 unmittelbar geltende EU Datenschutz-Grundverordnung (DSGVO) regelt in den Artikel 77 bis 84 DSGVO Rechtsbehelfe, Haftung und mögliche Sanktionen bei Verstößen gegen die DSGVO. Die Regelungen zu den Sanktionen und Rechtsbehelfen werden in den §§ 41 bis 44 des Bundesdatenschutzgesetzes konkretisiert. In den jeweiligen landesrechtlichen Datenschutzregelungen finden sich ebenfalls entsprechende Konkretisierungen.

17. Wird die Bundesregierung sich im Rahmen ihrer Beteiligungen dafür einsetzen, dass in der Aufarbeitung der vom CCC aufgedeckten Schwachstellen der Ausgabeverfahren die Einbeziehung der Expertise des Bundesbeauftragten für den Datenschutz nachgesucht wird, und wenn nein, warum nicht?

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wird bereits heute in alle Entscheidungen der Gesellschaft für Telematik mit Bezug zum Datenschutz eng einbezogen.

18. Hält die Bundesregierung den gesetzlichen Rahmen als auch die Informationen der verantwortlichen Stellen zur Sicherstellung ausschließlich autorisierter Herausgaben von Smart Cards und TI-Komponenten für ausreichend, und wenn nein, welche Änderungen und Anstöße plant sie zur Verbesserung der gegenwärtigen Situation?

Im Rahmen des Patientendaten-Schutzgesetzes beabsichtigt das Bundesministerium für Gesundheit die Sicherheit der Telematikinfrastruktur im Allgemeinen und die der Kartenausgabeprozesse im Besonderen weiter zu stärken. Geplant ist insbesondere, dass der Gesellschaft für Telematik eine zentrale Rolle bei der sicheren Ausgestaltung der Ausgabeprozesse übertragen wird und die Anforderungen an die Richtlinie nach § 217f SGB V verschärft werden.

19. Sind Bundesregierung, Gematik, Kartenherausgeber und Komponentenherausgeber oder Serviceprovider nach Kenntnis der Bundesregierung bislang auf die beim 36. Chaos Communication Congress in Leipzig zur Thematik vortragenden oder andere Mitglieder des Chaos Computer Clubs mit der Bitte um Austausch herangetreten?

    Wenn ja, wann, und mit welchem Ergebnis?

    Wenn nein, warum nicht?

Das Bundesministerium für Gesundheit und die Gesellschaft für Telematik standen zum Jahreswechsel im direkten Austausch mit Mitgliedern des Chaos Computer Clubs, um die Angriffe nachvollziehen und die notwendigen Maßnahmen ableiten zu können. Weitere Gespräche sind geplant.

Vorabfassung - wird durch die lektorierte Version ersetzt.

20. Plant die Bundesregierung angesichts der bekannt gewordenen Schwachstellen, die Vorgaben für dynamische Sicherheitsstandards zu erhöhen oder zu konkretisieren?

Die in der Telematikinfrastruktur zu verwendenden Sicherheitsstandards werden durch die Gesellschaft für Telematik in enger Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik nach dem Stand der Technik festgelegt, kontinuierlich geprüft und bei Bedarf angepasst.

21. Plant die Bundesregierung regelmäßige Pentests, Whitehacking-Programme, finanzierte Bugbounty-Programme oder vergleichbare Maßnahmen, um in Zukunft frühzeitig auf Sicherheitslücken der Telematikinfrastruktur aufmerksam zu werden?

Wenn ja, welche Überlegungen gibt es bereits hierzu auf Seiten der Bundesregierung oder nach Kenntnis der Bundesregierung auf Seiten der Gematik, Karten- und Komponentenherausgeber und Serviceprovider, wie werden solche Programme konkret ausgestaltet sein, und wann werden diese umgesetzt?

Wenn nein, warum nicht?

Die Bundesregierung sieht die Durchführung von regelmäßigen Penetrationstest als eine sehr gute Möglichkeit zur Überprüfung der bereits vorhanden und in Entwicklung befindlichen Software- und Hardwarekomponenten an. Im Kontext der Telematikinfrastruktur werden Penetrationstests mit spezialisierten externen Dienstleistern gegen alle Komponenten und Dienste der Telematikinfrastruktur durchgeführt.

Vorabfassung - wird durch die lektorierte Version ersetzt.

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