

**Änderungsantrag der Fraktionen der CDU/CSU und der SPD  
im 4. Ausschuss (Innenausschuss) des Deutschen Bundestages**

**zu dem Gesetzentwurf der Bundesregierung  
– Drucksache 16/11967 –  
Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik  
des Bundes**

Der Deutsche Bundestag wolle beschließen,  
den Gesetzentwurf der Bundesregierung - Drucksache 16/11967 - mit folgenden Maß-  
gaben, im Übrigen unverändert anzunehmen:

1. Artikel 1 wird wie folgt geändert:

a) § 5 wird wie folgt geändert:

aa) Absatz 2 wird wie folgt geändert:

aaa) Nach Satz 2 wird folgender Satz eingefügt:

„Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist.“

bbb) Nach dem neuen Satz 4 werden folgende Sätze eingefügt:

„Soweit hierzu die Wiederherstellung des Personenbezugs pseudonymisierter  
Daten erforderlich ist, muss diese durch den Präsidenten des Bundesamts an-  
geordnet werden. Die Entscheidung ist zu protokollieren.“

bb) Absatz 3 wird wie folgt gefasst:

„(3) Eine über die Absätze 1 und 2 hinausgehende Verwendung personenbezo-  
gener Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begrün-  
den, dass

1. diese ein Schadprogramm enthalten,
2. diese durch ein Schadprogramm übermittelt wurden oder
3. sich aus ihnen Hinweise auf ein Schadprogramm ergeben können,

und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen. Im Falle der Bestätigung ist die weitere Verarbeitung personenbezogener Daten zulässig, soweit dies

1. zur Abwehr des Schadprogramms,
2. zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen oder
3. zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.

Ein Schadprogramm kann beseitigt oder in seiner Funktionsweise gehindert werden. Die nicht automatisierte Verwendung der Daten nach den Sätzen 1 und 2 darf nur durch einen Bediensteten des Bundesamts mit der Befähigung zum Richteramt angeordnet werden.“

cc) Nach Absatz 3 wird folgender Absatz eingefügt:

„(4) Die Beteiligten des Kommunikationsvorgangs sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen, zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange Dritter entgegenstehen. Die Unterrichtung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde, und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat. Das Bundesamt legt Fälle, in denen es von einer Benachrichtigung absieht, dem behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem weiteren Bediensteten des Bundesamtes, der die Befähigung zum Richteramt hat, zur Kontrolle vor. Der behördliche Datenschutzbeauftragte ist bei Ausübung dieser Aufgabe weisungsfrei und darf deswegen nicht benachteiligt werden (§ 4f Absatz 3 des Bundesdatenschutzgesetzes). Wenn der behördliche Datenschutzbeauftragte der Entscheidung des Bundesamts widerspricht, ist die Be-

nachrichtigung nachzuholen. Die Entscheidung über die Nichtbenachrichtigung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist nach zwölf Monaten zu löschen. In den Fällen der Absätze 5 und 6 erfolgt die Benachrichtigung durch die dort genannten Behörden in entsprechender Anwendung der für diese Behörden geltenden Vorschriften. Enthalten diese keine Bestimmungen zu Benachrichtigungspflichten, sind die Vorschriften der Strafprozessordnung entsprechend anzuwenden.

dd) In dem neuen Absatz 5 Satz 1 werden die Wörter „einer Straftat von erheblicher Bedeutung oder einer mittels Telekommunikation begangenen Straftat“ durch die Wörter „einer mittels eines Schadprogramms begangenen Straftat nach den §§ 202a, 202b, 303a oder 303b des Strafgesetzbuches“ ersetzt.

ee) Der neue Absatz 6 wird wie folgt gefasst:

„Für sonstige Zwecke kann das Bundesamt die Daten übermitteln

1. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Absatz 2 der Strafprozessordnung bezeichneten Straftat,
2. an die Polizeien des Bundes und der Länder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist,
3. an die Verfassungsschutzbehörden des Bundes und der Länder, wenn tatsächliche Anhaltspunkte für Bestrebungen in der Bundesrepublik Deutschland vorliegen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Absatz 1 des Bundesverfassungsschutzgesetzes genannten Schutzgüter gerichtet sind.

Die Übermittlung nach Satz 1 Nummer 1 und 2 bedarf der vorherigen gerichtlichen Zustimmung. Für das Verfahren nach Satz 1 Nummer 1 und 2 gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den An-

gelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Zuständig ist das Amtsgericht, in dessen Bezirk das Bundesamt seinen Sitz hat. Die Übermittlung nach Satz 1 Nummer 3 erfolgt nach Zustimmung des Bundesministeriums des Innern; die §§ 9 bis 16 des Artikel 10-Gesetzes gelten entsprechend.“

ff) Der neue Absatz 7 wird wie folgt geändert:

aaa) Nach Satz 1 wird folgender Satz eingefügt:

„Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden.“

bbb) Der neue Satz 5 wird wie folgt gefasst:

„Dies gilt auch in Zweifelsfällen.“

ccc) Folgender Satz wird angefügt:

„Werden im Rahmen der Absätze 4 oder 5 Inhalte oder Umstände der Kommunikation von in § 53 Absatz 1 Satz 1 der Strafprozessordnung genannten Personen übermittelt, auf die sich das Zeugnisverweigerungsrecht der genannten Personen erstreckt, ist die Verwertung dieser Daten zu Beweis Zwecken in einem Strafverfahren nur insoweit zulässig, als Gegenstand dieses Strafverfahrens eine Straftat ist, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht ist.“

gg) In dem neuen Absatz 8 wird nach Satz 2 folgender Satz eingefügt:

„Die für die automatisierte Auswertung verwendeten Kriterien sind zu dokumentieren.“

hh) Folgende Absätze 9 und 10 werden angefügt:

„(9) Das Bundesamt unterrichtet den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über

1. die Anzahl der Vorgänge, in denen Daten nach Absatz 5 Satz 1, Absatz 5 Satz 2 Nummer 1 oder Absatz 6 Nummer 1 übermittelt wurden, aufgegliedert nach den einzelnen Übermittlungsbefugnissen,
2. die Anzahl der personenbezogenen Auswertungen nach Absatz 3 Satz 1, in denen der Verdacht widerlegt wurde,
3. die Anzahl der Fälle, in denen das Bundesamt nach Absatz 4 Satz 2 oder 3 von einer Benachrichtigung der Betroffenen abgesehen hat.

(10) Das Bundesamt unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Innenausschuss des Deutschen Bundestags über die Anwendung dieser Vorschrift.“

b) In § 6 Satz 3 wird die Angabe „6“ durch die Angabe „7“ ersetzt.

c) In § 7 Absatz 1 wird nach Satz 1 folgender Satz eingefügt:

„Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung von diese Produkte betreffenden Warnungen zu informieren, sofern hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks nicht gefährdet wird.“

d) § 8 Absatz 3 wird wie folgt geändert:

aa) Nach Satz 1 wird folgender Satz eingefügt:

„IT-Sicherheitsprodukte können nur in begründeten Ausnahmefällen durch eine Eigenentwicklung des Bundesamtes zur Verfügung gestellt werden.“

bb) In dem neuen Satz 7 wird die Angabe „4 und 5“ durch die Angabe „5 und 6“ ersetzt.

2. Artikel 3 wird aufgehoben.

3. Der bisherige Artikel 4 wird Artikel 3.

**Begründung:**

Zu Nummer 1

Zu Buchstabe a)

aa) Die nach Absatz 2 gespeicherten Protokolldaten sind durch technische und organisatorische Maßnahmen vor Missbrauch zu schützen. Hierzu gehört insbesondere, soweit mit vertretbarem Aufwand möglich, die Ersetzung von personenbezogenen Daten durch Pseudonyme. Dies ist insbesondere hinsichtlich der in den Protokolldaten enthaltenen Email-Adressen erforderlich, um die Erstellung von Kommunikationsprofilen zu verhindern. Um den Grundrechtseingriff nicht zu vertiefen, soll die Pseudonymisierung automatisiert erfolgen. Eine Entpseudonymisierung darf nur erfolgen, wenn dies für die Weiterverarbeitung nach Maßgabe der nachfolgenden Absätze erforderlich ist. Dies ist der Fall bei bestätigten Verdachtsfällen hinsichtlich eines Schadprogramms, um die Betroffenen warnen und erforderliche weitere Schutzmaßnahmen ergreifen zu können, sowie zur Erfüllung der Benachrichtigungspflichten nach Absatz 3. Die Entpseudonymisierung ist durch den Präsidenten anzuordnen und zu protokollieren. Technisch kann dies durch Verschlüsselung der entsprechenden Datenfelder erfolgen.

bb) Zur besseren Lesbarkeit wird der Absatz 3 in zwei Absätze aufgeteilt.

cc) Da es sich bei den Maßnahmen nach § 5 nicht um eine personen- oder inhaltsbezogene heimliche Überwachungsmaßnahmen handelt, sondern lediglich um eine weitgehend automatisierte Suche nach technischen Schadfunktionen, bedarf die Durchführung der Aufgabe selbst nicht der richterlichen Anordnung. Um stattdessen eine nachträgliche Kontrolle hinsichtlich der auch nicht-automatisiert verwendeten Daten zu ermöglichen, kommt der Benachrichtigung der Betroffenen eine besondere Bedeutung zu. Von der Benachrichtigung darf, wie auch nach § 101 Absatz 4 StPO, nur in besonderen Ausnahmefällen abgewichen werden. Diese Fälle sind dem be-

hördlichen Datenschutzbeauftragten sowie einem weiteren Mitarbeiter, der die Befähigung zum Richteramt hat, zur Kontrolle vorzulegen. Hält einer der beiden eine Benachrichtigung für erforderlich, kann er die zuständigen Mitarbeiter oder die Behördenleitung hiervon in Kenntnis setzen. Der behördliche Datenschutzbeauftragte ist nach § 4f Absatz 3 BDSG in der Ausübung seines Amtes unabhängig. Die Letztentscheidung liegt beim behördlichen Datenschutzbeauftragten. Die Zahl der Fälle, in denen von einer Benachrichtigung abgesehen wird, unterliegt der Unterrichtungspflicht nach den Absätzen 9 und 10. Die Nichtbenachrichtigung ist für die Zwecke der Datenschutzkontrolle durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit oder durch die Gerichte zu dokumentieren und zwölf Monate aufzubewahren. Diese Dokumentation darf nicht für andere Zwecke verwendet werden.

dd) Für die zweckbewahrende Übermittlung von Verdachtsfällen nach Absatz 5 sind, anders als im Fall des § 100g Absatz 1 StPO, nicht alle mittels Telekommunikation begangenen Straftaten, sondern nur die Straftatbestände der §§ 202a, 202b, 303a oder 303b StGB einschlägig, sofern sie mittels eines Schadprogramms begangen worden sind.

ee) Die Übermittlung von Zufallsfunden soll höheren Schranken unterworfen sein als die zweckbewahrende Übermittlung bei Schadprogrammfunden. Absatz 6 sieht daher zusätzliche Schranken, insbesondere einen Richtervorbehalt vor. Dieser Systematik soll auch die Übermittlung zu Strafverfolgungszwecken unterworfen werden. Daher wird die Übermittlungsbefugnis zur Verfolgung von Straftaten von erheblicher Bedeutung von Absatz 5 in Absatz 6 verschoben. Der Wortlaut entspricht § 100g Absatz 1 Nr. 1 StPO.

Die Änderung in Satz 2 dient der Klarstellung. Der Rechtsbegriff der Zustimmung umfasst im bürgerlichen Recht sowohl die Einwilligung (vorherige Zustimmung) als auch die Genehmigung (nachträgliche Zustimmung), vgl. Legaldefinitionen in § 183 Satz 1 und § 184 Absatz 1 BGB. Die Übermittlungsfälle des § 5 Absatz 6 bedürfen allerdings der vorherigen Zustimmung:

Da mit dem Auftreten erster Übermittlungsfälle aufgrund des voraussichtlichen Zeitpunktes des Inkrafttretens nicht vor Anfang September 2009 zu rechnen ist, kann sogleich und ausschließlich auf das FamFG verwiesen werden. Das FamFG tritt am 1. September 2009 in Kraft und löst das FGG ab.

- ff) Dass dem Bundesamt bei der Suche nach Schadprogrammen kernbereichsrelevante Inhalte zur Kenntnis gelangen, ist unwahrscheinlich. Soweit möglich, sollte schon technisch sichergestellt werden, dass diese nicht erhoben werden (so auch § 20k Absatz 7 Satz 2 BKAG). Um etwaige Eingriffe gleichwohl möglichst gering zu halten, sollen diese Inhalte unverzüglich gelöscht werden. Dies soll auch dann geschehen, wenn Zweifel bestehen, ob die Inhalte kernbereichsrelevant sind oder nicht. Für die Kommunikation von zeugnisverweigerungsberechtigten Berufsgruppen mit der Bundesverwaltung wird ein Beweisverwertungsverbot nach dem Vorbild des § 108 Absatz 3 StPO eingefügt. Anders als dort ist das Zeugnisverweigerungsrecht nicht auf Journalisten beschränkt.
- gg) Neben dem (abstrakten) Datenschutzkonzept sind auch die im Rahmen der automatisierten Auswertung konkret verwendeten Kriterien (Überprüfungsroutinen, Virensignaturen) zu dokumentieren.
- hh) Absatz 9 sieht zusätzliche Kontrollmöglichkeiten vor, indem eine Unterrichtspflicht über die Zahl der zweckändernden Übermittlungen, der Fehltreffer („false po-

sitives“) und der Fälle, in denen aufgrund der Ausnahmetatbestände des Absatzes 4 Satz 2 und 3 von einer Benachrichtigung der Betroffenen abgesehen wurde, gegenüber dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit geschaffen wird.

Außerdem soll das Bundesamt nach Absatz 10 jährlich den Innenausschuss umfänglich über die Umsetzung dieser Vorschrift, insbesondere die Bedrohungslage und die technische Entwicklung, unterrichten. Die Unterrichtung nach Absatz 10 beinhaltet auch die Zahlen nach Absatz 9.

Zu Buchstabe b)

Folgeänderung wegen der Absatzaufspaltung in § 5.

Zu Buchstabe c)

Nach dem in der IT-Wirtschaft geübten Prinzip der verantwortungsvollen Weitergabe („responsible disclosure“) werden in der Regel zunächst die Hersteller betroffener Produkte über entdeckte Sicherheitslücken informiert, um diesen Gelegenheit zu geben, Sicherheits-Updates zu entwickeln und ihren Kunden zur Verfügung zu stellen. Dieses Prinzip soll auch im Rahmen des § 7 Absatz 1 Beachtung finden. Eine Vorabinformation Dritter, insbesondere der Öffentlichkeit, ist allerdings dann geboten, wenn der Zweck der Maßnahme sonst nicht erreicht würde (vgl. § 40 Absatz 3 des Lebensmittel- und Futtermittelgesetzbuchs).

Zu Buchstabe d)

Aus Gründen der Wirtschaftlichkeit ist bei der Bereitstellung von IT-Sicherheitsprodukten grundsätzlich auf Produkte abzustellen, die am Markt erworben werden können. Spezifische Anforderungen der Verwaltung an Funktion und Sicherheit bestimmter Produkte haben allerdings teilweise zur Folge, dass keine geeigneten Produkte durch zuverlässige Hersteller am Markt angeboten werden. In solchen begrün-

deten Ausnahmefällen kann das Bundesamt auch entsprechende Produkte selber entwickeln.

Zu Nummer 2 und 3

Aufgrund der besonderen Eilbedürftigkeit der übrigen Regelungen des Gesetzentwurfs wird die Änderung des Telemedienrechts im Rahmen dieses Gesetzgebungsvorhabens nicht weiterverfolgt.