

**Gesetz**  
**zur Umsetzung der Richtlinie (EU) 2016/1148**  
**des Europäischen Parlaments und des Rates vom 6. Juli 2016**  
**über Maßnahmen zur Gewährleistung eines hohen gemeinsamen**  
**Sicherheitsniveaus von Netz- und Informationssystemen in der Union<sup>1</sup>**

Vom 23. Juni 2017

Der Bundestag hat das folgende Gesetz beschlossen:

**Artikel 1**

**Änderung des  
BSI-Gesetzes**

Das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 3 Absatz 6 des Gesetzes vom 18. Juli 2016 (BGBl. I S. 1666) geändert worden ist, wird wie folgt geändert:

1. § 2 wird wie folgt geändert:

a) Nach Absatz 10 wird folgender Absatz 11 eingefügt:

„(11) Digitale Dienste im Sinne dieses Gesetzes sind Dienste im Sinne von Artikel 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1), und die

1. es Verbrauchern oder Unternehmern im Sinne des Artikels 4 Absatz 1 Buchstabe a beziehungsweise Buchstabe b der Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die alternative Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG (Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten) (ABl. L 165 vom 18.6.2013, S. 63) ermöglichen, Kaufverträge oder Dienstleistungsverträge mit Unternehmern entweder auf der Webseite dieser Dienste oder auf der Webseite eines Unternehmers, die von diesen Diensten bereitgestellte Rechendienste verwendet, abzuschließen (Online-Marktplätze);

2. es Nutzern ermöglichen, Suchen grundsätzlich auf allen Webseiten oder auf Webseiten in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, die daraufhin

Links anzeigen, über die der Abfrage entsprechende Inhalte abgerufen werden können (Online-Suchmaschinen);

3. den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen (Cloud-Computing-Dienste),

und nicht zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden.“

b) Nach Absatz 11 wird folgender Absatz 12 angefügt:

„(12) „Anbieter digitaler Dienste“ im Sinne dieses Gesetzes ist eine juristische Person, die einen digitalen Dienst anbietet.“

2. § 3 Absatz 1 Satz 2 wird wie folgt geändert:

a) Nummer 13 Buchstabe b wird wie folgt geändert:

Nach dem Wort „Verfassungsschutzbehörden“ werden die Wörter „und des Militärischen Abschirmdienstes“ und nach dem Wort „Länder“ die Wörter „beziehungsweise dem Gesetz über den Militärischen Abschirmdienst“ eingefügt.

b) Nach Nummer 13 wird folgende Nummer 13a eingefügt:

„13a. auf Ersuchen der zuständigen Stellen der Länder Unterstützung dieser Stellen in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik;“.

c) Nummer 17 wird wie folgt geändert:

Die Angabe „und 8b“ wird durch die Angabe „bis 8c“ und der Punkt am Ende wird durch die Wörter „und digitaler Dienste;“ ersetzt.

d) Folgende Nummer 18 wird angefügt:

„18. Unterstützung bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen nach § 5a.“

3. § 5 wird wie folgt geändert:

a) Absatz 5 wird wie folgt geändert:

aa) In Satz 2 Nummer 2 werden nach dem Wort „Verfassungsschutz“ die Wörter „sowie an den Militärischen Abschirmdienst, wenn sich diese Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbe-

<sup>1</sup> Dieses Gesetz dient der Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

reich des Bundesministeriums der Verteidigung richten“ eingefügt.

bb) Es wird folgende Nummer 3 angefügt:

„3. zur Unterrichtung über Tatsachen, die einen internationalen kriminellen, terroristischen oder staatlichen Angriff mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland erkennen lassen, an den Bundesnachrichtendienst.“

b) Absatz 6 wird wie folgt geändert:

aa) Satz 1 wird wie folgt geändert:

aaa) In Nummer 3 werden nach dem Wort „Länder“ die Wörter „sowie an den Militärischen Abschirmdienst“ und nach dem Wort „Bundesverfassungsschutzgesetzes“ die Wörter „beziehungsweise § 1 Absatz 1 des Gesetzes über den Militärischen Abschirmdienst“ eingefügt.

bbb) Es wird folgende Nummer 4 angefügt:

„4. an den Bundesnachrichtendienst, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Straftaten nach § 3 Absatz 1 Nummer 8 des Artikel 10-Gesetzes plant, begeht oder begangen hat und dies von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland ist.“

bb) In Satz 5 wird nach der Angabe „Nummer 3“ die Angabe „und Nummer 4“ eingefügt.

4. Nach § 5 wird folgender § 5a eingefügt:

#### „§ 5a

Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen

(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Stelle oder des betroffenen Betreibers die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. Soweit das Bundesamt erste Maßnahmen zur Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort ergreift, werden hierfür keine Gebühren oder Auslagen für die Tätigkeit des Bundesamtes erhoben. Hiervon unberührt bleiben etwaige Kosten für die Hinzuziehung qualifizierter Dritter.

(2) Ein herausgehobener Fall nach Absatz 1 liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informa-

tionstechnischen Systems von besonderem öffentlichem Interesse ist.

(3) Das Bundesamt darf bei Maßnahmen nach Absatz 1 personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten erheben und verarbeiten, soweit dies zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich und angemessen ist. Die Daten sind unverzüglich zu löschen, sobald sie für die Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems nicht mehr benötigt werden. Wenn die Daten in Fällen des Absatzes 4 an eine andere Behörde zur Erfüllung von deren gesetzlichen Aufgaben weitergegeben worden sind, darf das Bundesamt die Daten abweichend von Satz 2 bis zur Beendigung der Unterstützung dieser Behörden weiterverarbeiten. Eine Nutzung zu anderen Zwecken ist unzulässig. § 5 Absatz 7 ist entsprechend anzuwenden. Im Übrigen sind die Regelungen des Bundesdatenschutzgesetzes anzuwenden.

(4) Das Bundesamt darf Informationen, von denen es im Rahmen dieser Vorschrift Kenntnis erlangt, nur mit Einwilligung des Ersuchenden weitergeben, es sei denn, die Informationen lassen keine Rückschlüsse auf die Identität des Ersuchenden zu oder die Informationen können entsprechend § 5 Absatz 5 und 6 übermittelt werden. Zugang zu den in Verfahren nach Absatz 1 geführten Akten wird Dritten nicht gewährt.

(5) Das Bundesamt kann sich bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden der Hilfe qualifizierter Dritter bedienen, wenn dies zur rechtzeitigen oder vollständigen Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich ist. Die hierdurch entstehenden Kosten hat der Ersuchende zu tragen. Das Bundesamt kann den Ersuchenden auch auf qualifizierte Dritte verweisen. Das Bundesamt und vom Ersuchenden oder vom Bundesamt nach Satz 1 beauftragte Dritte können einander bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden Daten übermitteln. Hierfür gilt Absatz 3 entsprechend.

(6) Soweit es zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems erforderlich ist, kann das Bundesamt vom Hersteller des informationstechnischen Systems verlangen, an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit mitzuwirken.

(7) In begründeten Einzelfällen kann das Bundesamt auch bei anderen als den in Absatz 1 genannten Einrichtungen tätig werden, wenn es darum ersucht wurde und es sich um einen herausgehobenen Fall im Sinne des Absatzes 2 handelt.

(8) Im Falle von Anlagen oder Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, ist in Fällen der Absätze 1, 4, 5 und 7 vor Tätigwerden des Bundesamtes das Benehmen mit den zuständigen atomrechtlichen Aufsichtsbehörden des Bundes und der Länder herzustellen. Im Falle von Anlagen oder Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, haben bei Maß-

nahmen des Bundesamtes nach § 5a die Vorgaben aufgrund des Atomgesetzes Vorrang.“

5. In § 7a Absatz 1 Satz 1 werden die Wörter „Nummer 1, 14 und 17“ durch die Wörter „Nummer 1, 14, 17 und 18“ ersetzt.

6. § 8a wird wie folgt geändert:

a) Absatz 3 wird wie folgt geändert:

aa) In Satz 3 werden die Wörter „eine Aufstellung“ durch die Wörter „die Ergebnisse“ ersetzt.

bb) Satz 4 wird durch die folgenden Sätze ersetzt:

„Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.“

b) Nach Absatz 3 wird folgender Absatz 4 eingefügt:

„(4) Das Bundesamt kann beim Betreiber Kritischer Infrastrukturen die Einhaltung der Anforderungen nach Absatz 1 überprüfen; es kann sich bei der Durchführung der Überprüfung eines qualifizierten unabhängigen Dritten bedienen. Der Betreiber Kritischer Infrastrukturen hat dem Bundesamt und den in dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Für die Überprüfung erhebt das Bundesamt Gebühren und Auslagen bei dem jeweiligen Betreiber Kritischer Infrastrukturen nur, sofern das Bundesamt auf Grund von Anhaltspunkten tätig geworden ist, die berechnete Zweifel an der Einhaltung der Anforderungen nach Absatz 1 begründeten.“

c) Der bisherige Absatz 4 wird Absatz 5.

7. § 8b wird wie folgt geändert:

a) Absatz 2 Nummer 4 wird wie folgt geändert:

aa) In Buchstabe b wird das Wort „sowie“ durch ein Komma ersetzt.

bb) In Buchstabe c wird das Wort „sowie“ angefügt.

cc) Folgender Buchstabe d wird angefügt:

„d) die zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union über nach Absatz 4 oder nach vergleichbaren Regelungen gemeldete erhebliche Störungen, die Auswirkungen in diesem Mitgliedstaat haben,“.

b) In Absatz 3 Satz 1 werden die Wörter „Kommunikationsstrukturen nach § 3 Absatz 1 Satz 2 Nummer 15“ durch die Wörter „von ihnen betriebenen Kritischen Infrastrukturen“ ersetzt.

c) Absatz 4 wird wie folgt geändert:

aa) Satz 1 wird wie folgt gefasst:

„Betreiber Kritischer Infrastrukturen haben die folgenden Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden:

1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,

2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.“

bb) Satz 2 wird wie folgt geändert:

aaa) Nach den Wörtern „Angaben zu der Störung“ werden die Wörter „, zu möglichen grenzübergreifenden Auswirkungen“ eingefügt.

bbb) Die Wörter „Branche des Betreibers“ werden durch die Wörter „erbrachten kritischen Dienstleistung und zu den Auswirkungen der Störung auf diese Dienstleistung“ ersetzt.

8. Nach § 8b wird folgender § 8c eingefügt:

„§ 8c

Besondere

Anforderungen an Anbieter digitaler Dienste

(1) Anbieter digitaler Dienste haben geeignete und verhältnismäßige technische und organisatorische Maßnahmen zu treffen, um Risiken für die Sicherheit der Netz- und Informationssysteme, die sie zur Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen, zu bewältigen. Sie haben Maßnahmen zu treffen, um den Auswirkungen von Sicherheitsvorfällen auf innerhalb der Europäischen Union erbrachte digitale Dienste vorzubeugen oder die Auswirkungen so gering wie möglich zu halten.

(2) Maßnahmen zur Bewältigung von Risiken für die Sicherheit der Netz- und Informationssysteme nach Absatz 1 Satz 1 müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Dabei ist folgenden Aspekten Rechnung zu tragen:

1. der Sicherheit der Systeme und Anlagen,
2. der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen,
3. dem Betriebskontinuitätsmanagement,
4. der Überwachung, Überprüfung und Erprobung,
5. der Einhaltung internationaler Normen.

Die notwendigen Maßnahmen werden durch Durchführungsrechtsakte der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 näher bestimmt.

(3) Anbieter digitaler Dienste haben jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb der Europäischen Union erbrachten digitalen Dienstes hat, unverzüglich dem Bundesamt zu melden. Die Voraussetzungen, nach denen Auswirkungen eines Sicherheitsvorfalls erheblich sind, werden durch Durchführungsakte der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 unter Berücksichtigung insbesondere der folgenden Parameter näher bestimmt:

1. die Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen,
2. die Dauer des Sicherheitsvorfalls,
3. das von dem Sicherheitsvorfall betroffene geographische Gebiet,
4. das Ausmaß der Unterbrechung der Bereitstellung des Dienstes,
5. das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.

Die Pflicht zur Meldung eines Sicherheitsvorfalls entfällt, wenn der Anbieter keinen ausreichenden Zugang zu den Informationen hat, die erforderlich sind, um die Auswirkung eines Sicherheitsvorfalls gemessen an den Parametern nach Satz 2 zu bewerten. Für den Inhalt der Meldungen gilt § 8b Absatz 3 entsprechend, soweit nicht Durchführungsakte der Kommission nach Artikel 16 Absatz 9 der Richtlinie (EU) 2016/1148 etwas anderes bestimmen. Über nach Satz 1 gemeldete Sicherheitsvorfälle, die Auswirkungen in einem anderen Mitgliedstaat der Europäischen Union haben, hat das Bundesamt die zuständige Behörde dieses Mitgliedstaats zu unterrichten.

(4) Liegen Anhaltspunkte dafür vor, dass ein Anbieter digitaler Dienste die Anforderungen des Absatzes 1 in Verbindung mit den Durchführungsrechtsakten der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 und des Absatzes 2 in Verbindung mit den Durchführungsrechtsakten der Kommission nach Artikel 16 Absatz 9 der Richtlinie (EU) 2016/1148 nicht erfüllt, kann das Bundesamt von dem Anbieter digitaler Dienste folgende Maßnahmen verlangen:

1. die Übermittlung der zur Beurteilung der Sicherheit seiner Netz- und Informationssysteme erforderlichen Informationen, einschließlich Nachweisen über ergriffene Sicherheitsmaßnahmen,
2. die Beseitigung von Mängeln bei der Erfüllung der in den Absätzen 1 und 2 bestimmten Anforderungen.

Die Anhaltspunkte können sich auch aus Feststellungen ergeben, die dem Bundesamt von den zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union vorgelegt werden.

(5) Hat ein Anbieter digitaler Dienste seine Hauptniederlassung, einen Vertreter oder Netz- und Informationssysteme in einem anderen Mitgliedstaat der Europäischen Union, so arbeitet das Bundesamt bei der Erfüllung der Aufgaben nach Absatz 4 mit der zuständigen Behörde dieses Mitgliedstaats zusammen. Diese Zusammenarbeit kann das Ersuchen umfassen, die Maßnahmen in Absatz 4 Satz 1 Nummer 1 und 2 zu ergreifen.“

9. Der bisherige § 8c wird § 8d und wird wie folgt geändert:

- a) In Absatz 1 Satz 2 werden nach der Angabe „Absatz 4“ die Wörter „des Anhangs“ eingefügt.
- b) Dem Absatz 2 Nummer 2 werden die Wörter „soweit sie den Regelungen des § 11 des Energiewirtschaftsgesetzes unterliegen,“ angefügt.
- c) Absatz 3 wird wie folgt geändert:
  - aa) In Nummer 2 werden die Wörter „im Sinne des Energiewirtschaftsgesetzes“ durch die Wörter „, soweit sie den Regelungen des § 11 des Energiewirtschaftsgesetzes unterliegen“ ersetzt.
  - bb) In dem Satzteil vor Nummer 1 und in Nummer 5 werden jeweils die Wörter „Absatz 3 bis 5“ durch die Angabe „Absatz 4“ ersetzt.

d) Folgender Absatz 4 wird angefügt:

„(4) § 8c Absatz 1 bis 3 gilt nicht für Kleinunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG. § 8c Absatz 3 gilt nicht für Anbieter,

1. die ihren Hauptsitz in einem anderen Mitgliedstaat der Europäischen Union haben oder
2. die, soweit sie nicht in einem Mitgliedstaat der Europäischen Union niedergelassen sind, einen Vertreter in einem anderen Mitgliedstaat der Europäischen Union benannt haben, in dem die digitalen Dienste ebenfalls angeboten werden.

Für Anbieter nach Satz 2 gilt § 8c Absatz 4 nur, soweit sie in der Bundesrepublik Deutschland Netz- und Informationssysteme betreiben, die sie zur Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen.“

10. Der bisherige § 8d wird § 8e und wird wie folgt geändert:

- a) Absatz 1 Satz 1 wird wie folgt geändert:
  - aa) Nach den Wörtern „§ 8a Absatz 2 und 3“ werden die Wörter „und § 8c Absatz 4“ und nach den Wörtern „§ 8b Absatz 4“ werden die Wörter „und § 8c Absatz 4“ eingefügt.
  - bb) Nach den Wörtern „Kritischer Infrastrukturen“ werden die Wörter „oder des Anbieters digitaler Dienste“ eingefügt.
  - cc) Das Wort „wesentlicher“ wird durch das Wort „von“ ersetzt und die Wörter „zu erwarten ist“ werden durch die Wörter „eintreten kann“ ersetzt.

b) Absatz 2 wird wie folgt gefasst:

„(2) Zugang zu den Akten des Bundesamtes in Angelegenheiten nach den §§ 8a bis 8c wird

bei Vorliegen der Voraussetzungen des § 29 des Verwaltungsverfahrensgesetzes nur gewährt, wenn schutzwürdige Interessen des betroffenen Betreibers Kritischer Infrastrukturen oder des Anbieters digitaler Dienste dem nicht entgegenstehen und durch den Zugang zu den Akten keine Beeinträchtigung von Sicherheitsinteressen eintreten kann.“

c) Folgender Absatz 3 wird angefügt:

„(3) Für Betreiber nach § 8d Absatz 2 und 3 gelten die Absätze 1 und 2 entsprechend.“

11. Dem § 10 wird folgender Absatz 4 angefügt:

„(4) Soweit die Durchführungsrechtsakte der Kommission nach Artikel 16 Absatz 8 und 9 der Richtlinie (EU) 2016/1148 keine abschließenden Bestimmungen über die von Anbietern digitaler Dienste nach § 8c Absatz 2 zu treffenden Maßnahmen oder über die Parameter zur Beurteilung der Erheblichkeit der Auswirkungen von Sicherheitsvorfällen nach § 8c Absatz 3 Satz 2 oder über Form und Verfahren der Meldungen nach § 8c Absatz 3 Satz 4 enthalten, werden diese Bestimmungen vom Bundesministerium des Innern im Einvernehmen mit den jeweils betroffenen Ressorts durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, getroffen.“

12. In § 11 wird die Angabe „§ 5“ durch die Wörter „die §§ 5 und 5a“ ersetzt.

13. Dem § 13 werden die folgenden Absätze 3 bis 5 angefügt:

„(3) Das Bundesamt übermittelt bis zum 9. November 2018 und danach alle zwei Jahre die folgenden Informationen an die Kommission:

1. die nationalen Maßnahmen zur Ermittlung der Betreiber Kritischer Infrastrukturen;
2. eine Aufstellung der im in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, die nach § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrad;
3. eine zahlenmäßige Aufstellung der Betreiber der in Nummer 2 genannten Sektoren, die in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren ermittelt werden, einschließlich eines Hinweises auf ihre Bedeutung für den jeweiligen Sektor.

Die Übermittlung darf keine Informationen enthalten, die zu einer Identifizierung einzelner Betreiber führen können. Das Bundesamt übermittelt die nach Satz 1 übermittelten Informationen unverzüglich dem Bundesministerium des Innern, dem Bundeskanzleramt, dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit.

(4) Sobald bekannt wird, dass eine Einrichtung oder Anlage nach § 2 Absatz 10 oder Teile einer Einrichtung oder Anlage eine wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistung in einem der in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren in einem anderen Mitgliedstaat der Europäischen Union bereitstellt, nimmt das Bundesamt zum Zweck der gemeinsamen Ermittlung der Betreiber, die kritische Dienstleistungen in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Teilsektoren erbringen, mit der zuständigen Behörde dieses Mitgliedstaats Konsultationen auf.

(5) Das Bundesamt übermittelt bis zum 9. August 2018 und danach jährlich an die Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 einen zusammenfassenden Bericht zu den Meldungen, die die in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren oder digitale Dienste betreffen. Der Bericht enthält auch die Zahl der Meldungen und die Art der gemeldeten Sicherheitsvorfälle sowie die ergriffenen Maßnahmen. Der Bericht darf keine Informationen enthalten, die zu einer Identifizierung einzelner Meldungen oder einzelner Betreiber oder Anbieter führen können.“

14. § 14 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Nummer 2 werden die Wörter

„Satz 4

a) Nummer 1 oder

b) Nummer 2“

durch die Angabe „Satz 5“ ersetzt.

bb) In Nummer 3 wird das Wort „oder“ am Ende durch ein Komma ersetzt.

cc) In Nummer 4 wird der Punkt am Ende durch ein Komma ersetzt.

dd) Die folgenden Nummern 5 bis 7 werden angefügt:

„5. entgegen § 8c Absatz 1 Satz 1 eine dort genannte Maßnahme nicht trifft,

6. entgegen § 8c Absatz 3 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vornimmt oder

7. einer vollziehbaren Anordnung nach § 8c Absatz 4

a) Nummer 1 oder

b) Nummer 2

zuwiderhandelt.“

b) Dem Absatz 2 wird folgender Satz angefügt:

„In den Fällen des Absatzes 1 Nummer 5 bis 7 wird die Ordnungswidrigkeit nur geahndet, wenn der Anbieter digitaler Dienste seine Hauptniederlassung nicht in einem anderen Mitgliedstaat der Europäischen Union hat oder, soweit er nicht in einem anderen Mitgliedstaat der Europäischen Union niedergelassen ist, dort einen Vertreter benannt hat und in diesem Mitgliedstaat dieselben digitalen Dienste anbietet.“

15. Folgender § 15 wird angefügt:

„§ 15

Anwendbarkeit der  
Vorschriften für Anbieter digitaler Dienste

Die Vorschriften, die Anbieter digitaler Dienste betreffen, sind ab dem 10. Mai 2018 anwendbar.“

**Artikel 2**

**Änderung des  
Atomgesetzes**

§ 44b des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 1 des Gesetzes vom 1. Juni 2017 (BGBl. I S. 1434) geändert worden ist, wird wie folgt geändert:

1. In Satz 2 werden die Wörter „§ 8b Absatz 1, 2 und Absatz 7“ durch die Wörter „§ 8b Absatz 1, 2 Nummer 1 bis 3, Nummer 4 Buchstabe a bis c und Absatz 7“ ersetzt.
2. In Satz 4 werden nach den Wörtern „des Bundes und des Landes“ die Wörter „und an die von diesen bestimmten Sachverständigen nach § 20“ eingefügt.

**Artikel 3**

**Änderung des  
Energiewirtschaftsgesetzes**

Das Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 24 Absatz 28 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1693) geändert worden ist, wird wie folgt geändert:

1. § 11 Absatz 1c wird wie folgt gefasst:

„(1c) Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben

1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage geführt haben,
2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können,

über die Kontaktstelle unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik zu melden.

Die Meldung muss Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und der betroffenen Informationstechnik, enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktions-

fähigkeit der Kritischen Infrastruktur geführt hat. Das Bundesamt für Sicherheit in der Informationstechnik hat die Meldungen unverzüglich an die Bundesnetzagentur weiterzuleiten. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird. Zugang zu den Akten des Bundesamtes für Sicherheit in der Informationstechnik sowie zu den Akten der Bundesnetzagentur in Angelegenheiten nach § 11 Absatz 1a bis Absatz 1c wird nicht gewährt. § 29 des Verwaltungsverfahrensgesetzes bleibt unberührt. § 8e Absatz 1 des BSI-Gesetzes ist entsprechend anzuwenden.“

2. § 95 wird wie folgt geändert:

- a) In Absatz 1 werden nach Nummer 2 folgende Nummern 2a und 2b eingefügt:

„2a. entgegen § 11 Absatz 1a oder 1b den Katalog von Sicherheitsanforderungen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig einhält,

2b. entgegen § 11 Absatz 1c eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vornimmt,“.

- b) Absatz 5 wird wie folgt gefasst:

„(5) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist in den Fällen des Absatzes 1 Nummer 2b das Bundesamt für Sicherheit in der Informationstechnik, im Übrigen die nach § 54 zuständige Behörde.“

**Artikel 4**

**Änderung des  
Fünften Buches Sozialgesetzbuch**

Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch Artikel 7 des Gesetzes vom 23. Mai 2017 (BGBl. I S. 1228) geändert worden ist, wird wie folgt geändert:

1. Dem § 291b wird folgender Absatz 8 angefügt:

„(8) Die Gesellschaft für Telematik legt dem Bundesamt für Sicherheit in der Informationstechnik auf Verlangen die folgenden Unterlagen und Informationen vor:

1. die Zulassungen und Bestätigungen nach den Absätzen 1a bis 1c und 1e einschließlich der zugrunde gelegten Dokumentation,
2. eine Aufstellung der nach den Absätzen 6 und 7 getroffenen Maßnahmen einschließlich der festgestellten Sicherheitsmängel und Ergebnisse der Maßnahmen und
3. sonstige für die Bewertung der Sicherheit der Telematikinfrastruktur sowie der zugelassenen Dienste und bestätigten Anwendungen erforderlichen Informationen.

Ergibt die Bewertung der in Satz 1 genannten Informationen Sicherheitsmängel, so kann das Bundesamt für Sicherheit in der Informationstechnik der Gesellschaft für Telematik verbindliche Anweisungen zur Beseitigung der festgestellten Sicherheitsmängel

erteilen. Die Gesellschaft für Telematik ist befugt, Betreibern von zugelassenen Diensten und bestätigten Anwendungen nach den Absätzen 1a bis 1c und 1e verbindliche Anweisungen zur Beseitigung festgestellter Sicherheitsmängel zu erteilen. Die Kosten der Überprüfung tragen

1. die Gesellschaft für Telematik, sofern das Bundesamt für Sicherheit in der Informationstechnik auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Sicherheit der Telematikinfrastruktur begründeten,
2. der Betreiber von zugelassenen Diensten und bestätigten Anwendungen nach den Absätzen 1a bis 1c und 1e, sofern das Bundesamt für Sicherheit in der Informationstechnik auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Sicherheit der zugelassenen Dienste und bestätigten Anwendungen begründeten.“

2. § 307 wird wie folgt geändert:

- a) Nach Absatz 1 werden folgende Absätze 1a bis 1c eingefügt:

„(1a) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 291b Absatz 6 Satz 2 und 4 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vornimmt.

(1b) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 291b Absatz 8 Satz 2 einer verbindlichen Anweisung nicht, nicht vollständig oder nicht rechtzeitig Folge leistet.

(1c) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 291b Absatz 8 Satz 3 einer verbindlichen Anweisung nicht, nicht vollständig oder nicht rechtzeitig Folge leistet.“

- b) Folgender Absatz 4 wird angefügt:

„(4) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist in den Fällen der Absätze 1a bis 1c das Bundesamt für Sicherheit in der Informationstechnik.“

## Artikel 5

### Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 22 Absatz 3 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1822) geändert worden ist, wird wie folgt geändert:

1. § 100 Absatz 1 wird wie folgt geändert:

- a) In Satz 1 werden nach den Wörtern „der Teilnehmer und Nutzer“ die Wörter „sowie die Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind,“ eingefügt.
- b) Nach Satz 1 wird folgender Satz eingefügt:

„Die Kommunikationsinhalte sind nicht Bestandteil der Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung.“

c) Die folgenden Sätze werden angefügt:

„Die Daten sind unverzüglich zu löschen, sobald sie für die Beseitigung der Störung nicht mehr erforderlich sind. Eine Nutzung der Daten zu anderen Zwecken ist unzulässig. Soweit die Daten nicht automatisiert erhoben und verwendet werden, muss der betriebliche Datenschutzbeauftragte unverzüglich über die Verfahren und Umstände der Maßnahme informiert werden. Der Diensteanbieter muss dem betrieblichen Datenschutzbeauftragten, der Bundesnetzagentur und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am Ende eines Quartals detailliert über die Verfahren und Umstände von Maßnahmen nach Satz 6 in diesem Zeitraum schriftlich berichten. Die Bundesnetzagentur leitet diese Informationen unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik weiter. Der Betroffene ist von dem Diensteanbieter zu benachrichtigen, sofern dieser ermittelt werden kann. Wurden im Rahmen einer Maßnahme nach Satz 1 auch Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung erhoben und verwendet, müssen die Berichte mindestens auch Angaben zum Umfang und zur Erforderlichkeit der Erhebung und Verwendung der Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung enthalten.“

2. § 109 Absatz 5 wird wie folgt geändert:

- a) In Satz 1 werden nach dem Wort „Bundesnetzagentur“ die Wörter „und dem Bundesamt für Sicherheit in der Informationstechnik“ eingefügt.
- b) Satz 5 wird aufgehoben.
- c) In dem neuen Satz 7 wird die Angabe „§ 8d“ durch die Angabe „§ 8e“ ersetzt.

3. § 109a wird wie folgt geändert:

- a) Dem Absatz 4 wird folgender Satz angefügt:

„Der Diensteanbieter darf die Teile des Datenverkehrs von und zu einem Nutzer, von denen eine Störung ausgeht, umleiten, soweit dies erforderlich ist, um den Nutzer über die Störungen benachrichtigen zu können.“

- b) Nach Absatz 4 werden die folgenden Absätze 5 und 6 eingefügt:

„(5) Der Diensteanbieter darf im Falle einer Störung die Nutzung des Telekommunikationsdienstes bis zur Beendigung der Störung einschränken, umleiten oder unterbinden, soweit dies erforderlich ist, um die Beeinträchtigung der Telekommunikations- und Datenverarbeitungssysteme des Diensteanbieters, eines Nutzers im Sinne des Absatzes 4 oder anderer Nutzer zu beseitigen oder zu verhindern und der Nutzer die Störung nicht unverzüglich selbst beseitigt oder zu erwarten ist, dass der Nutzer die Störung selbst nicht unverzüglich beseitigt.

(6) Der Diensteanbieter darf den Datenverkehr zu Störungsquellen einschränken oder unterbinden, soweit dies zur Vermeidung von Störungen

in den Telekommunikations- und Datenverarbeitungssystemen der Nutzer erforderlich ist.“

c) Der bisherige Absatz 5 wird Absatz 7.

4. § 149 wird wie folgt geändert:

a) Nach Absatz 1 Nummer 17b werden die folgenden Nummern 17c und 17d eingefügt:

„17c. entgegen § 100 Absatz 1 Satz 3 die Daten nicht oder nicht rechtzeitig löscht,

17d. entgegen § 100 Absatz 1 Satz 4 die Daten zu anderen Zwecken genutzt werden,“.

b) Die bisherige Nummer 17c wird Nummer 17e.

#### **Artikel 6**

#### **Inkrafttreten**

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

---

Die verfassungsmäßigen Rechte des Bundesrates sind gewahrt.

Das vorstehende Gesetz wird hiermit ausgefertigt. Es ist im Bundesgesetzblatt zu verkünden.

Berlin, den 23. Juni 2017

Der Bundespräsident  
Steinmeier

Die Bundeskanzlerin  
Dr. Angela Merkel

Der Bundesminister des Innern  
Thomas de Maizière