Recht der Informationssicherheit

Kipker / Reusch / Ritter

2023
ISBN 978-3-406-78339-5
C.H.BECK

B. Einzelerläuterungen

I. Ausnahmen zum Recht auf Löschung (Abs. 1)

S. 1 räumt dem BSI die Möglichkeit ein, **einem Löschungsbegehren** einer betroffenen Person nach Art. 17 DS-GVO **nicht nachzukommen,** wenn die personenbezogenen Daten **nicht automatisiert verarbeitet werden, eine Löschung** wegen der besonderen Art der Speicherung **nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und das Interesse der betroffenen Person an der Löschung als gering anzusehen ist.** Damit wird dem Aufwand Rechnung getragen, der insbesondere entsteht, wenn größere Mengen an Daten nicht automatisiert gespeichert werden und damit nicht ohne weiteres durchsuchbar sind. Der vertretbare Aufwand soll sich, ähnlich wie in § 35 BDSG,[3] nach dem jeweiligen **Stand der Technik** bemessen und insbesondere nicht oder nur mit unverhältnismäßig hohem Aufwand veränderbare oder löschbare Datenspeicher betreffen.[4] Weiterhin muss eine **Feststellung des Interesses** der betroffenen Person stattfinden. Nur wenn dieses Interesse **zusätzlich zum hohen Aufwand des BSI,** dem Löschungsersuchen nachzugehen, als gering anzusehen ist, darf auf die Löschung verzichtet werden. **2**

Die Einschränkung des Rechts auf Löschung gemäß Art. 17 DS-GVO dient dem Schutz eines wichtigem **Ziels des allgemeinen öffentlichen Interesses,** nämlich des der **Gewährleistung der Funktionsfähigkeit und Aufgabenerledigung der öffentlichen Verwaltung** gemäß Art. 23 Abs. 1 lit. e DS-GVO,[5] damit diese durch das Löschbegehren nicht an **Kapazitätsgrenzen** gebracht wird. **3**

Sollte das BSI einem Löschungsersuchen aufgrund von S. 1 nicht nachkommen, so muss es jedenfalls nach **S. 2** eine **Einschränkung der Verarbeitung gemäß Art. 18 DS-GVO** vornehmen. Einschränkung der Verarbeitung in diesem Sinne meint dabei eine „Markierung gespeicherter personenbezogener Daten, mit dem Ziel, ihre künftige Verarbeitung einzuschränken" gemäß Art. 4 Nr. 3 DS-GVO. Die **DS-GVO** nennt in **Erwgr. 67** selbst **Beispiele,** mit welchen Methoden eine solche Einschränkung vorgenommen werden kann. Demnach können bspw. ausgewählte personenbezogene Daten vorübergehend auf ein anderes Verarbeitungssystem übertragen werden, die Verarbeitung kann für Nutzer gesperrt werden oder bspw. veröffentlichte Daten von einer Webseite entfernt werden. Diese Beschränkung wird damit auch **Art. 23 Abs. 2 lit. c DS-GVO** gerecht, der für Beschränkungen der Betroffenenrechte entsprechende **Schutzmaßnahmen** verlangt. Im Übrigen sind durch den Verweis auf Art. 18 DS-GVO insgesamt auch die **Art. 18 Abs. 2 und 3 DS-GVO** anwendbar, welche mit einer **strengen Zweckbindung** der in der Verarbeitung eingeschränkten Daten (Art. 18 Abs. 2 DS-GVO) und einer **Unterrichtungspflicht der betroffenen Person** (Art. 18 Abs. 3 DS-GVO) ebenfalls **Schutzmaßnahmen** im Sinne von Art. 23 Abs. 2 lit. a, c, d und h DS-GVO vorsehen.[6] **4**

Für den Fall, dass sich bei der Prüfung des Löschbegehrens herausstellt, dass die personenbezogenen Daten der betroffenen Person bereits **unrechtmäßig ver-** **5**

[3] BT-Drs. 18/11325, 105.
[4] BT-Drs. 19/4674, 216.
[5] BT-Drs. 19/4674, 216.
[6] Vgl. auch BT-Drs. 18/11325, 105 zum teilweise wortgleichen § 35 BDSG.

arbeitet wurden, müssen die Daten regelmäßig gelöscht werden. **S. 1 und S. 2 sind nicht anzuwenden,** da ein **Verantwortlicher in diesem Fall nicht schutzwürdig** ist und der entsprechende Aufwand dann abverlangt werden kann.[7]

II. Fälle von § 5 Abs. 3, Einschränkung der Verarbeitung (Abs. 2)

6 Nach **S. 1** dürfen personenbezogen Daten, die nur **aufgrund einer etwaigen gerichtlichen Überprüfung nach § 5 Abs. 3 nicht gelöscht werden,** ohne weitere Einwilligung der betroffenen Person auch ausschließlich **nur zu diesem Zweck verwendet werden** und sind **im Übrigen in der Verarbeitung einzuschränken. S. 2** stellt weiterhin ausdrücklich klar, dass **§ 5 Abs. 7,** der ebenfalls eine **Zweckbindung** hinsichtlich der nach § 5 zu verarbeiteten Daten vorsieht, unberührt bleibt. Beide Sätze waren in § 6 aF, der sich ausschließlich auf die Löschung von personenbezogenen Daten bezog, bereits enthalten und sollten beibehalten werden.[8] Gleichzeitig stellen sie aber auch weitere Ausprägungen der **Schutzmaßnahmen nach Art. 23 Abs. 2 lit. a, c, d DS-GVO** dar.

§ 6e Recht auf Einschränkung der Verarbeitung

Die Pflicht des Bundesamtes zur Einschränkung der Verarbeitung gemäß Artikel 18 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 besteht für die Dauer der Überprüfung der Richtigkeit der personenbezogenen Daten nicht, wenn

1. **die Verarbeitung oder Weiterverarbeitung durch dieses Gesetz ausdrücklich geregelt ist oder**
2. **die Einschränkung der Verarbeitung die Abwehr von Gefahren für die Sicherheit in der Informationstechnik gefährden würde**

und deswegen das Interesse der betroffenen Person an der Einschränkung zurücktreten muss.

Literatur: *Kipker,* Endlich Datenschutz im BSIG? – Referentenentwurf für ein Gesetz zur Anpassung des bereichsspezifischen Datenschutzes und zur Umsetzung der EU JI-Richtlinie (2. DSAnpUG-EU), ZD-Aktuell 2018, 04317.

A. Allgemeines

1 § 6e[1] sieht die Möglichkeit für das BSI vor, einem **Ersuchen der betroffenen Person auf Einschränkung der Verarbeitung** ihrer personenbezogenen Daten für die Dauer der Überprüfung der Richtigkeit dieser Daten **nicht nachzukommen** für den Fall, dass diese von der betroffenen Person bestritten wird. Damit stellt die Regelung eine **Ausnahme zu Art. 18 Abs. 1 lit. a DS-GVO** dar.

2 Anders als bei §§ 6a, 6b, 6d sehen **weder Art. 18 DS-GVO noch §§ 32 ff. BDSG eigene Ausnahmen des Rechts der betroffenen Person auf Einschränkung der Verarbeitung** vor. Einschränkungen sind jedoch nach **§ 27 Abs. 2 BDSG,** der die Einschränkung der Betroffenenrechte bei der Datenver-

[7] BT-Drs. 19/4674, 216; dies entspricht der Fallgruppe des Art. 17 Abs. 1 lit. d DS-GVO.
[8] BT-Drs. 19/4674, 216.
[1] Zum Hintergrund der Einführung der §§ 6 ff. → § 6 Rn 1 ff.

arbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken regelt, sowie nach **§ 28 Abs. 4 BDSG,** der die Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken regelt, möglich, da diese Sachverhalte nicht im BSIG geregelt werden, vgl. § 6 BSIG iVm § 1 Abs. 2 BDSG.

B. Einzelerläuterungen

Gemäß § 6e besteht das **Recht der betroffenen Person auf Einschränkung der Verarbeitung** ihrer personenbezogenen Daten **nicht** für den Fall, dass sie die Richtigkeit dieser Daten bestreitet, wenn entweder **die (Weiter-)Verarbeitung dieser Daten nach dem BSIG ausdrücklich geregelt ist (Nr. 1) oder die Einschränkung der Verarbeitung die Abwehr von Gefahren für die Sicherheit in der Informationstechnik gefährden würde (Nr. 2).** In beiden Fällen muss aufgrund des Vorliegens dieser Tatbestandsmerkmale das **Interesse der betroffenen Person** an der Einschränkung **zurücktreten.** **3**

Die Regelung dient ausweislich der Gesetzesbegründung der Sicherstellung der nationalen und der öffentlichen Sicherheit und dem Schutz sonstiger wichtiger **Ziele des allgemeinen öffentlichen Interesses gemäß Art. 23 Art. 1 lit a, c und e DS-GVO.**[2] Die Beschränkung des Rechts der betroffenen Person gemäß Art. 18 DS-GVO sei erforderlich, da anderenfalls die **Aufgabenwahrnehmung des BSI erheblich gefährdet** würde, wenn zunächst die Daten der betroffenen Person ggf. mit unverhältnismäßigem Aufwand ermittelt und überprüft werden müssten und solange nicht weiter verwendet werden könnten.[3] Solche Daten werden oft automatisiert verarbeitet und sind einer natürlichen Person teilweise überhaupt nur unter hohem Aufwand zuzuordnen (zB bei IP-Adressen). Daher könnte die Suspendierung der Verarbeitung faktisch zum Stillstand der Verarbeitung und damit zu **erheblichen Schutzlücken der Sicherheit in der Informationstechnik**[4] führen. **4**

Wann konkret die (Weiter-)Verarbeitung von personenbezogenen Daten nach **Nr. 1** im BSIG ausdrücklich geregelt ist und damit kein Recht auf Einschränkung der Verarbeitung besteht, dazu verhält sich die Norm nicht. Durch die Bezugnahme auf **„ausdrücklich“** kann davon ausgegangen werden, dass nicht die „normale“ Aufgabenerfüllung gemeint ist, mit der ggf. eine Verarbeitung personenbezogener Daten einhergeht, vgl. § 3a Abs. 1 iVm § 3. Dies würde anderenfalls praktisch jede Verarbeitung von personenbezogenen Daten durch das BSI umfassen, weswegen es des Einschubs des Wortes „ausdrücklich“ nicht bedurft hätte. Weiterhin würde hierdurch die Ausnahmeregelung deutlich ausgeweitet, was wiederum Fragen nach der Verhältnismäßigkeit dieser Alternative aufwerfen würde. Insofern erscheint es sachgerechter, Nr. 1 **nur auf die Tatbestände im BSIG anzuwenden, in denen ausdrücklich die (Voraussetzungen und Grenzen einer) Verarbeitung personenbezogener Daten geregelt ist,** bspw. nach § 5. **5**

Nach **Nr. 2** besteht weiterhin **kein Recht der betroffenen Person auf Einschränkung der Verarbeitung** ihrer personenbezogenen Daten, wenn dies die **Abwehr von Gefahren für die Sicherheit in der Informationstechnik** gefährden würde. **„Sicherheit in der Informationstechnik“** ist definiert in § 2 Abs. 2 **6**

---

[2] BT-Drs. 19/4674, 216.
[3] BT-Drs. 19/4674, 216.
[4] BT-Drs. 19/4674, 216.

und meint die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in und bei Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen. Damit findet Nr. 2 den Bezugspunkt für die Gefahr in der Terminologie des BSIG selbst, anders als § 6a und § 6b, die sich mit der „Gewährleistung der Netz- und Informationssicherheit" an der Terminologie der DS-GVO in Erwgr. 49 orientieren und für die es jedenfalls keine gesetzlich vorgegebene Definition gibt. In welchen **Beispielsfällen** eine Verarbeitung von personenbezogenen Daten nicht während der Dauer der Überprüfung ihrer Richtigkeit aufgrund von Gefahren für die Sicherheit in der Informationstechnik eingeschränkt werden kann, führen **weder das Gesetz noch die Gesetzesbegründung** auf.[5] Denkbar ist dies aber beispielsweise im Rahmen einer Verarbeitung nach § 5, wo die Einschränkung der Verarbeitung personenbezogener Daten während der Überprüfung ihrer Richtigkeit dazu führen könnte, dass die dauerhaft ausgeführte und automatisierte Abwehr von Schadprogrammen und anderen Gefahren für die Kommunikationstechnik des Bundes insgesamt unterbrochen werden müsste, während die Richtigkeit einzelner Datensätze überprüft wurde. Derartige Einzelfälle könnten demnach tatsächlich zu erheblichen Schutzlücken in der Sicherheit der Informationstechnik[6] führen.

§ 6f Widerspruchsrecht

[1]Das Recht der betroffenen Person auf Widerspruch gemäß Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 besteht nicht, wenn

1. **an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder**
2. **eine Rechtsvorschrift das Bundesamt zur Verarbeitung verpflichtet.**

[2]Darüber hinaus darf das Bundesamt die personenbezogenen Daten ergänzend zu Artikel 21 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 so lange verarbeiten, bis das Bundesamt geprüft hat, ob zwingende schutzwürdige Gründe für die Verarbeitung bestehen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.

Literatur: *Kipker,* Endlich Datenschutz im BSIG? – Referentenentwurf für ein Gesetz zur Anpassung des bereichsspezifischen Datenschutzes und zur Umsetzung der EU JI-Richtlinie (2. DSAnpUG-EU), ZD-Aktuell 2018, 04317.

A. Allgemeines

1 Nach **Art. 21 DS-GVO** hat die betroffene Person **das Recht, der Verarbeitung ihrer personenbezogenen Daten zu widersprechen,** wenn diese auf **Grundlage des Art. 6 Abs. 1 UAbs. 1 lit. e oder f DS-GVO** geschieht und **besondere Gründe für die Nichtverarbeitung** in ihrer Person gegeben sind. In der Konsequenz darf ein Verantwortlicher bei Vorliegen dieses Tatbestands die per-

[5] Daher wird dieser Tatbestand auch als zu weitgehend kritisiert, s. *Kipker,* ZD-Aktuell 2018, 04317.

[6] BT-Drs. 19/4674, 216.

sonenbezogenen Daten dieser Person dann grundsätzlich nicht mehr verarbeiten. **§ 6f**[1] **schließt** in den dort genannten Fallalternativen **dieses Recht der betroffenen Person aus.**

Eigene Ausnahmen zum Widerspruchsrecht der betroffenen Person **sieht Art. 21 DS-GVO nicht vor.** Jedoch findet sich eine **Ausnahmeregelung** in **§ 36 BDSG,** zu dem § 6f inhaltlich gleich geregelt wurde. § 36 BDSG wäre allerdings ohnehin nur anwendbar, wenn dies nach § 6 BSIG und § 1 Abs. 2 BDSG zulässig wäre oder wenn sich die Datenverarbeitung außerhalb des Anwendungsbereichs der DS-GVO bewegt, § 1 Abs. 8 BDSG. Grundsätzlich anwendbar hingegen werden sein **§ 27 Abs. 2 BDSG,** der die Einschränkung der Betroffenenrechte bei der Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken regelt, sowie **§ 28 Abs. 4 BDSG,** der die Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken regelt. Beide Sachverhalte werden nicht im BSIG geregelt, sodass die ergänzenden Regelungen des BDSG greifen können, vgl. § 6 BSIG iVm § 1 Abs. 2 BDSG. 2

B. Einzelerläuterungen

Nach S. 1 besteht **das Recht** der betroffenen Person **auf Widerspruch** gegen die Verarbeitung ihrer personenbezogenen Daten gemäß Art. 21 DS-GVO **nicht, wenn an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt (S. 1 Nr. 1) oder eine Rechtsvorschrift das BSI** zu Verarbeitung dieser Daten **verpflichtet (S. 1 Nr. 2).** 3

Ein öffentliches Interesse an der Verarbeitung nach **S. 1 Nr. 1** kann regelmäßig **bei jeder Aufgabenwahrnehmung des BSI angenommen werden,** da § 3 Abs. 1 S. 2 nunmehr bestimmt, dass sämtliche Aufgaben des BSI solche im öffentlichen Interesse sind. Wann jedoch ein **„zwingendes" öffentliches Interesse** besteht, dazu verhält sich weder § 6f noch die Gesetzesbegründung. **Unklar** verbleibt damit, ob das Merkmal „zwingend" ein **eigenständiges Tatbestandsmerkmal** darstellen soll oder lediglich eine Art ‚Redaktionsversehen', welches gleichwohl bei jedweder Aufgabenerfüllung nach § 3 Abs. 1 S. 2 gegeben ist. Der unterschiedliche Gebrauch der ‚öffentlichen Interessen' im BSIG und auch der im Übrigen uferlos weit erscheinende Anwendungsbereich dieser eigentlichen Ausnahmeregelung sprechen jedoch für Ersteres,[2] so dass zunächst **immer eine Prüfung** stattfinden muss, **ob** die streitige Verarbeitung tatsächlich **ein zwingend zu erfüllendes öffentliches Interesse** verfolgt, **welches dann zusätzlich auch die Interessen der betroffenen Person am Widerspruch überwiegt.** Welche **Kriterien** hierfür gelten sollen, lässt das Gesetz jedoch **offen.** Eine Konkretisierung des Prüfungsmaßstabs wäre vor dem Hintergrund der Einschränkung von Betroffenenrechten und auch für die Erleichterung der Rechtsanwendung wünschenswert gewesen. Klarer ist insoweit **S. 1 Nr. 2,** der das Recht auf Widerspruch ebenfalls ausschließt, wenn das BSI durch Rechtsvorschrift zur Verarbeitung verpflichtet ist.[3] 4

Art. 21 Abs. 1 S. 2 DS-GVO schränkt das Recht der betroffenen Person auf Widerspruch zudem insoweit ein, als dass **ein Verantwortlicher die Verarbei-** 5

[1] Zum Hintergrund der Einführung der §§ 6ff. → § 6 Rn 1ff.
[2] So auch *Kipker,* ZD-Aktuell 2018, 04317.
[3] Vgl. bspw. § 8 Abs. 3.

tung ihrer Daten nicht einstellen muss, wenn er **zwingende schutzwürdige Gründe für die Verarbeitung nachweisen** kann, **die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen. S. 2** gestattet es dem BSI zusätzlich hierzu, die personenbezogenen Daten der betroffenen Person **so lange weiter zu verarbeiten, bis diese Prüfung abgeschlossen ist.** Hintergrund ist hier, dass insbesondere bei bestimmten Aufgaben des BSI, bspw. nach §§ 5, 5a,[4] große Datenmengen vorhanden sind, die teilweise automatisiert verarbeitet werden. Diese automatisierte Verarbeitung müsste ggf. unterbrochen werden für den Zeitraum, in dem das BSI prüft, ob die zwingenden, schutzwürdigen Gründe für die Verarbeitung bestehen, die auch die Interessen der betroffenen Person überwiegen. Dies könnte zu Schutzlücken und einer Gefährdung der Netz- und Informationssicherheit in diesem Rahmen führen, wenn die Verarbeitung zwischenzeitlich ausgesetzt werden müsste.[5] Diese Argumentation trifft jedoch sicherlich nicht auf jede Aufgabenwahrnehmung des BSI zu, weswegen jedenfalls eine **einschränkende Auslegung und Anwendung auf bestimmte, vergleichbar (zeit-)kritische Verarbeitungsgrundlagen im BSIG anzudenken** ist, um den Rechten und Interessen der betroffenen Person gerecht zu werden.

6 Vor diesem Hintergrund erscheint auch das Stützen der Grundlage der Beschränkung nach § 6 f insgesamt auf **Art. 23 Abs. 1 lit. a, c und e DS-GVO**[6] recht pauschal und weit gefasst, da jedenfalls für S. 2 eine differenziertere Auseinandersetzung mit den einzelnen Aufgaben erforderlich gewesen wäre.

§ 7 Warnungen

(1) **[1]Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 und 14 a kann das Bundesamt**

1. die folgenden Warnungen und Informationen an die Öffentlichkeit oder an die betroffenen Kreise richten:
   a) Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten,
   b) Warnungen vor Schadprogrammen,
   c) Warnungen bei einem Verlust oder einem unerlaubten Zugriff auf Daten und
   d) Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten.
2. Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen.

[2]Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist.

(1 a) **[1]Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung der Warnungen zu informieren. [2]Diese Informationspflicht besteht nicht,**

1. wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet wird oder

---

[4] Vgl. BT-Drs. 19/4674, 217.
[5] Vgl. BT-Drs. 19/4674, 217.
[6] BT-Drs. 19/4674, 217, kritisch auch *Kipker,* ZD-Aktuell 2018, 04317.

2. wenn berechtigterweise davon ausgegangen werden kann, dass der Hersteller an einer vorherigen Benachrichtigung kein Interesse hat.

[3]Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen einschränken. [4]Kriterien für die Auswahl des zu warnenden Personenkreises nach Satz 3 sind insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers.

(2) **[1]Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 und 14a kann das Bundesamt die Öffentlichkeit unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts und Dienstes vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen warnen, wenn hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik hiervon ausgehen, oder Sicherheitsmaßnahmen sowie den Einsatz bestimmter informationstechnischer Produkte und Dienste empfehlen. [2]Stellen sich die an die Öffentlichkeit gegebenen Informationen im Nachhinein als falsch oder die zugrunde liegenden Umstände als unzutreffend wiedergegeben heraus, ist dies unverzüglich öffentlich bekannt zu machen.**

Literatur: *Augsberg,* Informationsverwaltungsrecht, 2014; *Becker,* Gemeinschaftsrechtliche Zulässigkeit staatlicher Produktinformationen und -empfehlungen, EuR 2002, 418; *Buchberger,* Die Aufgaben des Bundesamts für Sicherheit in der Informationstechnik nach den Änderungen des BSIG 2015 bis 2017 – ein Überblick, GSZ 2019, 183; *v. Danwitz,* Verfassungsfragen staatlicher Produktempfehlungen, 2003; *Bundesamt für Sicherheit in der Informationstechnik (BSI),* Die Lage der IT-Sicherheit in Deutschland 2020, https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html; *Dietrich,* Der Einsatz von Verschlüsselungstechniken zwischen Grundrechtsschutz und staatlicher Sicherheitsgewährleistung, GSZ 2021, 1; *Feik,* Öffentliche Verwaltungskommunikation, 2007; *Gehrmann/Voigt,* IT-Sicherheit – Kein Thema nur für Betreiber Kritischer Infrastrukturen, CR 2017, 93; *Gusy,* Verwaltung durch Information – Empfehlungen und Warnungen als Mittel des Verwaltungshandelns, NJW 2000, 977; *Gusy,* Neutralität staatlicher Öffentlichkeitsarbeit – Voraussetzungen und Grenzen, NVwZ 2015, 700; *Herpig,* Schwachstellen-Management für mehr Sicherheit, 2018, https://www.stiftung-nv.de/sites/default/files/vorschlag.schwachstellenmanagement.pdf; *Hornung/Schallbruch* (Hrsg.), IT-Sicherheitsrecht, 2021; *Hornung,* Neue Pflichten für Betreiber kritischer Infrastrukturen: Das IT-Sicherheitsgesetz des Bundes, NJW 2015, 3334; *Hornung,* Das IT-Sicherheitsgesetz 2.0: Kompetenzaufwuchs des BSI und neue Pflichten für Unternehmen, NJW 2021, 1985; *Hufen/Siegel,* Fehler im Verwaltungsverfahren, 6. Aufl. 2018; *Ingold,* Desinformationsrecht: Verfassungsrechtliche Vorgaben für staatliche Desinformationstätigkeit, 2011; *Kloepfer,* Staatliche Informationen als Lenkungsmittel, 1998; *Kopp/Ramsauer* (Hrsg.), Verwaltungsverfahrensgesetz: VwVfG, 21. Aufl. 2020; *Kugelmann* (Hrsg.), Migration, Datenübermittlung und Cybersicherheit, 2016; *Leisterer,* Internetsicherheit in Europa – Zur Gewährleistung der Netz- und Informationssicherheit durch Informationsverwaltungsrecht, 2018; *Leisterer/Schneider,* Staatliches Informationshandeln im Bereich der IT-Sicherheit, K&R 2015, 681; *Meyer/Streinz* (Hrsg.), LFGB BasisVO HCVO, 2. Aufl. 2012; *Ossenbühl/Cornils,* Staatshaftungsrecht, 6. Aufl. 2013; *Ritter* (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2022; *Raue,* Haftung für unsichere Software, NJW 2017, 1841; *Roos,* Das IT-Sicherheitsgesetz – Wegbereiter oder Tropfen auf den heißen Stein?, MMR 2015, 636; *Schallbruch,* IT-Sicherheits-

recht – Abwehr von IT-Angriffen, Haftung und Ausblick, CR 2018, 215; *Schenke/Graulich/Ruthig* (Hrsg.), Sicherheitsrecht des Bundes, 2. Aufl. 2019; *Schieble,* Öffentliche Warnungen vor unsicheren Verbraucherprodukten: Behördliche Befugnisse und Haftungsrecht, VuR 2007, 401; *Schmidt-Kessel,* Für ein digitales Produktsicherheitsrecht – ein Plädoyer, VuR 2015, 121; *Schneider,* Meldepflichten im IT-Sicherheitsrecht – Datenschutz, Kritische Infrastrukturen und besondere IT-Dienste, 2017; *Seckelmann/Lamping,* Verhaltensökonomischer Experimentalismus im Politik-Labor – Rechtliche Rahmenbedingungen und Folgerungen für die Evaluationsforschung, DÖV 2016, 189; *Spindler,* IT-Sicherheitsgesetz und zivilrechtliche Haftung, CR 2016, 297; *Stelkens/Bonk/Sachs* (Hrsg.), VwVfG: Verwaltungsverfahrensgesetz, 9. Aufl. 2018; *Tremml/Luber,* Amtshaftungsansprüche wegen rechtswidriger Produktinformation, NJW 2005, 1745; *Meisterernst/Sosnitza* (Hrsg.), Zipfel/Rathke, Lebensmittelrecht, 178. EL 2020.

Inhaltsübersicht

A. Allgemeines

I. Zweck und Entstehung der Vorschrift

1 Das BSI hat mit § 7 die Kompetenz, gesetzlich näher bestimmte **Warnungen** an die Öffentlichkeit oder betroffene Kreise zu richten und diese Adressatenkreise zu **informieren.** Wenn auch nicht von der Überschrift erfasst, beinhaltet § 7 auch die Befugnis, bestimmte **Empfehlungen** auszusprechen. Die Vorschrift gehört damit zum Nukleus des digitalen Produktsicherheitsrechts.[1] Mit der Befugnis kann das BSI die weit gefassten Aufgaben nach § 3 Abs. 1 S. 2 Nr. 14 und Nr. 14a erfüllen.

2 Während die Befugnis in der 2009 geschaffenen Fassung mit der Möglichkeit zur Warnung der Öffentlichkeit einen vordergründig vorsorgenden Charakter hatte, wurde mit der Erweiterung durch das IT-SiG von 2015 die **gefahrenabwehrrechtliche Stoßrichtung** der Norm gestärkt.[2] Die Befugnis wurde erneut 2021

[1] *Schmidt-Kessel,* VuR 2015, 121 (122).
[2] *Schallbruch,* CR 2018, 215 (217).