**Deutscher Bundestag**
Innenausschuss

Ausschussdrucksache
18(4)278

# Stellungnahme

## des Gesamtverbandes der Deutschen Versicherungswirtschaft

## zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

## - BT-Drs. 18/4096 -

Gesamtverband der Deutschen
Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020-5000
Fax: +49 30 2020-6000

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +32 2 28247-39
ID-Nummer 6437280268-55

Ansprechpartner:
Dr. Axel Wehling,
Mitglied der Hauptgeschäftsführung

Fred Chiachiarella
Leiter Betriebswirtschaft / Informations-technologie

E-Mail: a.wehling@gdv.de
f.chiachiarella@gdv.de

www.gdv.de

## Inhaltsübersicht



### Zusammenfassung

Für die Versicherungswirtschaft sind ein sicherer Rechtsrahmen und abgesicherte IT-Infrastrukturen von grundsätzlicher Bedeutung. Die technischen und rechtlichen Rahmenbedingungen müssen so weiterentwickelt werden, dass sie den wachsenden Ansprüchen von Bürgerinnen und Bürgern und damit auch Kunden, Behörden und Dienstleistern entsprechen. Der Verband begrüßt daher, dass die Bundesregierung mit dem vorgelegten Entwurf einen wichtigen Schritt in Richtung IT-Sicherheit und vor allem Rechtssicherheit gehen möchte.

Hervorzuheben ist insbesondere die Unterstreichung des kooperativen Ansatzes und die Stärkung der sogenannten Single Point of Contacts (SPOCs) der Branchen. Änderungen sollten noch im Bereich der Meldepflichten erfolgen. So sollten die Meldungen, die keine Nennung des betroffenen Betreibers erfordern, nicht pseudonymisiert, sondern anonymisiert und sicher über die SPOCs erfolgen.

Insbesondere muss sichergestellt werden, dass durch mögliche Spezialgesetzgebung keine dezentralen Meldestrukturen geschaffen werden, die die Möglichkeiten der schnellen und fachkundigen Analyse und unverzügliche Weiterleitung an das Bundesamt stark beeinträchtigen würden.

## 1. Einleitung

Der Gesamtverband der Deutschen Versicherungswirtschaft begrüßt die Schwerpunktsetzung auf IT-Sicherheit in der Digitalen Agenda und die Fortführung der Initiative der Bundesregierung, mit dem Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) nicht nur IT-Sicherheit, sondern vor allem auch Rechtssicherheit zu schaffen.

Die Versicherungswirtschaft ist einer der Wirtschaftszweige, der mit als erster die Digitalisierung aufgegriffen und vorangetrieben hat. Sie ist nicht nur Nutzer neuer Informations- und Kommunikationstechnologien, sondern auch Impulsgeber für Innovationen und für die Stärkung der Informationsgesellschaft. Die verantwortungsvolle Verarbeitung umfangreicher und oft sensibler Daten ist daher die Basis eines erfolgreichen Versicherungsgeschäfts, IT- und Datensicherheit sind für die Versicherungswirtschaft Kernanliegen.

Zum jetzt vorliegenden Regierungsentwurf (Stand: 17. Dezember 2014) möchten wir wie folgt Stellung nehmen:

## 2. Artikel 1: Änderung des BSI-Gesetzes

### 2.1. § 3 Abs. 1 BSIG

*Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es folgende Aufgaben wahr:*
*[…]*

*2. Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, sowie für Dritte, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist;*

*[…]*

*15. Aufbau geeigneter Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zum Schutz der Sicherheit in der Informationstechnik Kritischer Infrastrukturen im Verbund mit der Privatwirtschaft;*

*16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland, unbeschadet besonderer Zuständigkeiten anderer Stellen;*

17. *Aufgaben nach den §§ 8a und 8b als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen.*

Die hierdurch dem Bundesamt eingeräumte Möglichkeit, wichtige Informationen zu kritischen IT-Vorfällen auch an Dritte weitergeben zu können, wird generell begrüßt.

Hier bedarf es jedoch aus Sicht der Versicherungswirtschaft einer weiteren Konkretisierung der „Dritten“, an die die vom BSI gewonnenen Erkenntnisse weitergegeben werden dürfen. Insbesondere ist nicht klar, wer im Sinne der Begründung zum „Bereich der Kritischen Infrastrukturen im weiteren Sinne“ gehören soll. Das Gesetz dient ja gerade der Abgrenzung zwischen solchen Bereichen, die zu diesen Infrastrukturen gehören und anderen, bei denen das gerade nicht der Fall ist. Von einer dritten Kategorie ist im Gesetz nicht die Rede.

Bei der Weitergabe von Informationen, insbesondere an Dritte, ist weiterhin darauf zu achten, dass ein Rückschluss auf das möglicherweise betroffene Unternehmen und die Branche hierbei nicht möglich ist.

### 2.2. § 2 Abs. 10 BSIG i.V.m. § 10 Abs. 1 BSIG

*§ 2 Abs. 10 BSIG*
*Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die*

1. *den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und*
2. *von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.*

*Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.*

*§ 10 Abs. 1 BSIG*
*Das Bundesministerium des Innern bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit 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 unter Festlegung der in den jeweiligen Sektoren im Hinblick auf § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt."*

Die Versicherungswirtschaft begrüßt auch in diesem Punkt den kooperativen Ansatz zur Feststellung derjenigen Dienstleistungen und Systeme, die Gegenstand des Gesetzes sein sollen. Die Beteiligung der betroffenen Betreiber bei der Konkretisierung der Kriterien für Kritische Infrastrukturen darf sich nicht auf die in § 10 Abs. 1 vorgesehen Anhörung beschränken. Erforderlich ist vielmehr die auch in der Begründung angesprochene konkrete Einbeziehung bei der Entwicklung einer branchenspezifischen Definition von Qualität und Quantität. Gerade mit Blick auf den immensen Aufwand, der für den Nachweis der angemessenen organisatorischen und technischen Vorkehrungen gemäß § 8a Abs. 1, 3 BSIG und die Meldepflichten nach § 8b Abs. 4 BSIG notwendig ist, ist eine Regulierung mit Augenmaß notwendig, die vor allem Rechtssicherheit schafft.[1]

### 2.3. § 8a Abs. 1, 3 BSIG

*Absatz 1:*
*Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei ist der Stand der Technik zu berücksichtigen. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.*

*Absatz 3:*
*Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre*

[1] Siehe hierzu auch Punkt 2.7

*die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.*

Der Nachweis der Vorkehrungen aus Absatz 1 („angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse“) gemäß Absatz 3 ist so gefasst, dass den betroffenen Unternehmen der erforderliche Gestaltungsrahmen zur Verfügung steht und eine verantwortliche Umsetzung möglich ist.

Die Definition von „Sicherheitsaudits, Prüfungen oder Zertifizierungen“ (Absatz 3, Satz 2) sollte geschärft werden. Unklar ist, ob interne Sicherheitsaudits / Prüfungen durch entsprechend zertifizierte Mitarbeiter des jeweiligen Unternehmens (z. B. innerhalb der Revision) als Nachweis ausreichend sind oder ob es zwingend eines Nachweises durch Externe bedarf. Sofern eine gültige Zertifizierung nach einem anerkannten Standard vorhanden ist (z. B. ISO 27001), dürfen keine weiteren Audits notwendig sein. Des Weiteren ist nicht klar definiert, ob die gesamte IT-Infrastruktur der Unternehmen oder nur die Teile überprüft bzw. zertifiziert werden müssen, die zur Aufrechterhaltung der Funktionsfähigkeit notwendig sind.

Weiterhin wird in Absatz 3, Satz 4 festgeschrieben, dass bei der Entdeckung von jedweden Sicherheitsmängeln die Übermittlung der gesamten Prüfungsunterlagen zu erfolgen hat. Dies ist aus Sicht der Versicherungswirtschaft unverhältnismäßig und kontraproduktiv, da Ziel dieser Prüfungen ja gerade das Beheben etwaiger Schwachstellen und das Entdecken von Verbesserungspotenzial in der Systemsicherheit ist. Hier sollte die Meldung auf erhebliche Mängel, die zum Ausfall der informationstechnischen Systeme führen kann, beschränkt werden. Es scheint außerdem wenig zielführend, dass die zu meldenden Störungen nach § 8b Abs. 4 eine gewisse Schwelle überschreiten müssen, Prüfberichte aber bereits bei kleinsten Mängeln vollständig vorgelegt werden müssen. Eine dementsprechende Klarstellung sollte in den Gesetzestext mit aufgenommen

werden.

### 2.4. § 8a Abs. 2 BSIG

*Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt*

> *1. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,*
> *2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde.*

Der Verband befürwortet explizit den hier festgeschriebenen kooperativen und verantwortlichen Ansatz, der bereits in den letzten Jahren aktiv im Umsetzungsplan KRITIS (UP KRITIS) − auch mit seinen Branchenarbeitskreisen als „etablierte Kooperationsplattform“[2] − erfolgreich installiert wurde. Als Grundlage für die branchenspezifischen Standards sollten hier bereits bestehende und anerkannte Standards (beispielsweise ISO 27001 oder BSI-Grundschutz) dienen, um eine Synchronisierung mit bereits existierenden Anforderungen zu erreichen und damit den administrativen und organisatorischen Aufwand für die Unternehmen so gering wie möglich zu halten. Der Verband wird sich in diesen Prozess konstruktiv und zielorientiert einbringen.

### 2.5. § 8b Abs. 4 BSIG

*Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder bereits geführt haben, über die Kontaktstelle unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und zur Branche des Betreibers enthalten. Die Nennung des Betrei-*

[2] Regierungsentwurf zum IT-Sicherheitsgesetz vom 17. Dezember 2014, Gesetzesbegründung, S. 15, dritter Absatz

*bers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.*

Der Verband begrüßt, dass mit „erheblichen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit“ eine gegenüber dem Referentenentwurf deutlich verbesserte Definition gefunden wurde, die zusammen mit der höchstrichterlichen Rechtsprechung zu § 100 Abs. 1 TKG und den Klarstellungen in der Begründung zur Frage der Erheblichkeit eine rechtssichere Grundlage für das weitere Verfahren darstellen kann.

Der Verband befürwortet außerdem, dass die Meldepflicht weiterhin in mehreren Stufen erfolgen soll und dass „Die Nennung des Betreibers […] nur dann erforderlich [ist], wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.“ Jedoch ist laut Gesetzesbegründung vorgesehen, dass diese Meldungen pseudonymisiert und nicht anonymisiert erfolgen soll. Wenn von einer Pseudonymisierung nicht abgewichen werden kann, muss durch ein geeignetes Verfahren sichergestellt werden, dass die Pseudoidentität von den Branchenansprechpartnern so gewählt wird, dass ein Rückschluss auf das meldende Unternehmen nicht möglich ist. Meldungen sollten dabei aber in den meisten Fällen anonym erfolgen, da vor allem ein nationales Lagebild erstellt werden soll.

Nach der Gesetzesbegründung sollen zur weiteren Konkretisierung der Meldepflicht „das BSI − unter Einbeziehung der Betreiber Kritischer Infrastrukturen und der ansonsten im Bereich der Sicherheitsvorsorge zuständigen Aufsichtsbehörden − Kriterien für meldungsrelevante Sicherheitsvorfälle aufstellen und entsprechend der jeweils aktuellen IT-Sicherheitslage weiterentwickeln.“[3] Eine Abstimmung mit den betroffenen Branchen erscheint insbesondere an dieser Stelle unerlässlich, da nur diese qualifiziert die Auswirkungen einer Beeinträchtigung oder eines Ausfalls beurteilen können.

### 2.6. § 8b Abs. 5 BSIG

*Zusätzlich zu ihrer Kontaktstelle nach Absatz 3 können Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, eine gemeinsame übergeordnete Ansprechstelle benennen. Wurde eine solche*

[3] Regierungsentwurf zum IT-Sicherheitsgesetz vom 17. Dezember 2014, Gesetzesbegründung Seite 20, 2. Absatz

*benannt, erfolgt der Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt in der Regel über die gemeinsame Ansprechstelle.*

Die durch diese Regelung vorgenommene Stärkung der sogenannten Single Point of Contacts (SPOCs), die neben den Kontaktstellen der Betreiber als übergeordnete Ansprechstelle benannt werden können, ist besonders positiv hervorzuheben. Dies wird zu einer verkürzten Kommunikation zwischen den Branchen und dem Bundesamt führen und damit insbesondere auch zu schnelleren Reaktionszeiten in Krisenfällen. Aber auch für kleine Versicherungsunternehmen, die von den Reglungen nicht betroffen sind, ist ein solcher Branchenansprechpartner als Bindeglied zu den zuständigen Behörden sinnvoll.

Bereits im Jahr 2010 wurde von der Versicherungswirtschaft das Krisenreaktionszentrum für IT-Sicherheit der deutschen Versicherungswirtschaft GmbH (LKRZV) gegründet. Es erfüllt bereits jetzt die Forderung der Bundesregierung, im IT-Krisenfall die Reaktions- und Kommunikationsfähigkeit innerhalb der Branche und mit den zuständigen Behörden sicherzustellen.

Dass die Regelkommunikation über die gemeinsame Ansprechstelle erfolgen soll, wird ausdrücklich begrüßt. Dafür ist es aus Sicht des Verbandes notwendig und bisher auch geübte Praxis, dass die SPOCs als gemeinsame Ansprechstelle den Inhalt der Meldungen kennen, um ggf. eine brancheninterne Betroffenheit, z. B. durch mehrere vergleichbare Warnmeldungen aus verschiedenen Unternehmen, schnell erkennen zu können und dem Bundesamt eine entsprechende Einschätzung mitzugeben. Damit werden die SPOCs in die Lage versetzt, branchenspezifische Warnungen an ihre Mitgliedsunternehmen zu verschicken, um unabhängig von der Analyse des Bundesamtes bereits im Vorfeld die IT-Sicherheit der Branche zu stärken.

### 2.7. § 8 c Abs. 1 BSIG

*Die §§ 8a und 8b sind nicht anzuwenden auf Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36). Artikel 3 Absatz 4 der Empfehlung ist nicht anzuwenden.*

Diese Regelung stellt sicher, dass insbesondere kleinere Unternehmen durch Administrationskosten und Kosten für den Nachweis der technischen und organisatorischen Vorkehrungen nach § 8a Abs. 1, 3 BSIG

nicht unverhältnismäßig belastet werden.[4] Auch diese Regelung wird daher ausdrücklich begrüßt. Schließlich ist festzustellen, dass auch die nicht betroffenen Versicherungsunternehmen selbstverständlich höchste Anforderungen an ihre IT-Sicherheit erfüllen.

Zu Rückversicherungen ist festzustellen, dass diese der Risikobewältigung einzelner Versicherungsunternehmen dienen und daher per se nicht als Kritische Infrastruktur eingestuft werden können. In der Versicherungsbranche sind nur Erstversicherungen als kritisch anzusehen, da nur diese im direkten Kontakt mit den Verbrauchern stehen. Dies gilt umso mehr, wenn die Rückversicherer keinen Hauptsitz in Deutschland haben.

### 2.8. § 8c Abs. 2, 3 BSIG

*Absatz 2:*
*§ 8a ist nicht anzuwenden auf […]*
*4. sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8a vergleichbar oder weitergehend sind.*

*Absatz 3:*
*§ 8b Absatz 3 bis 5 ist nicht anzuwenden auf […]*
*4. sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8b Absatz 3 bis 5 vergleichbar oder weitergehend sind.*

Nach den hier vorliegenden Normen besteht die Möglichkeit, Spezialregelungen zu schaffen, die das gesamte etablierte und gut funktionierende bidirektionale Warn- und Meldesystem zwischen dem Bundesamt und den SPOCs, das in den §§ 8a und 8b Abs. 3 bis 5 BSIG ausgeführt wird, aushebeln würde.

Der Verband hat bereits in seinen Stellungnahmen zu den Referentenentwürfen aus den Jahren 2013 und 2014 hervorgehoben, dass der Erhalt bewährter Warn- und Meldewege notwendig ist. Bei der Krisenkommunikation ist es essentiell, dass diese direkt, schnell und zielgerichtet zwischen Experten erfolgt. Gewonnene Erkenntnisse müssen gerade bei relevanten IT-Sicherheitsvorfällen schnellstmöglich ausgetauscht werden, um drohenden Schäden erfolgreich entgegenwirken zu können.

Die Versicherungswirtschaft verfügt mit dem LKRZV bereits über eine

[4] Siehe hierzu auch Punkt 2.1

sichere und bewährte zentrale Kommunikationsinfrastruktur mit dem Bundesamt. Hinzu kommt, dass das Bundesamt auch in der Vergangenheit immer wieder unter Beweis gestellt hat, dass es über die fachliche und technische Kompetenz verfügt, Meldungen schnell einzuordnen, die notwendigen Schritte zum Schutz aller Kritischen Infrastrukturen einzuleiten und gegebenenfalls den betroffenen Unternehmen und Branchen über die SPOCs Hilfe anzubieten.

Hier dezentrale Meldestrukturen für die Versicherungsunternehmen über die Aufsichtsbehörde BaFin (zum Bundesamt) einzuführen, würde nicht nur den Alarmierungsweg unnötig verlängern und damit den Schaden möglicherweise vergrößern, sondern auch verhindern, dass Sicherheitswarnungen branchenübergreifend und schnellstmöglich versandt werden können. Dem Anspruch des IT-Sicherheitsgesetzes, die IT-Sicherheitslage für ganz Deutschland zu verbessern, würde diese Regelung nicht gerecht werden.

Es würde außerdem dazu führen, dass die Aufsicht über die Kritischen Infrastrukturen in verschiedene Aufsichtsbereiche (bspw. Bundesamt für Verkehr oder Bundesamt für Ernährung und Landwirtschaft) zerfasert und damit einen erheblichen Bedeutungsverlust erleiden würde. Die Erstellung eines einheitlichen Lagebildes − die in § 8b Abs. 2 Nr. 3 BSIG als Aufgabe des Bundesamtes explizit genannt wurde − und schnelle Reaktionen, die allen Betreibern Kritischer Infrastrukturen zugutekommen würden, wären so praktisch unmöglich.

Der Verband plädiert daher weiterhin für die ersatzlose Streichung in beiden Absätzen ab „sowie“ („…sowie sonstige Betreiber Kritischer Infrastrukturen, die aufgrund von Rechtsvorschriften vergleichbare oder weitergehende Anforderungen ….“).

Alternativ besteht die Möglichkeit, dass Aufsichtsbehörden die Informationen über Vorfälle aus den entsprechenden Branchen über das Bundesamt erhalten. Das Bundesamt könnte somit die Rolle eines „Behörden-SPOC“ einnehmen, die ihm in § 8b Abs. 1 BSIG („zentrale Meldestelle für Betreiber Kritischer Infrastrukturen“) auch explizit eingeräumt wird. Durch dieses Verfahren könnte das Bundesamt außerdem gemeinsam mit den „Branchen-SPOCs“ zu einem effizienten und möglichst unbürokratischen Verfahren beitragen. So kann auch das Interesse der Betreiber Kritischer Infrastrukturen, einen einzigen und schnellen Warn- und Meldeweg zu einer kompetenten Behörde zu haben, in Einklang gebracht werden.

## 2.9. § 8d BSIG

*Absatz 1:*
*Das Bundesamt kann Dritten auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3 erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4 nur erteilen, wenn schutzwürdigen Interessen des betroffenen Betreibers Kritischer Infrastrukturen dem nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen zu erwarten ist. Zugang zu personenbezogenen Daten wird nicht gewährt.*

*Absatz 2:*
*Zugang zu den Akten des Bundesamtes in Angelegenheiten nach den §§ 8a und 8b wird nur Verfahrensbeteiligten gewährt und dies nach Maßgabe von § 29 des Verwaltungsverfahrensgesetzes.*

Diese Regelung ist als Lex Specialis zum Informationsfreiheitsgesetz (IFG) anzusehen. Bei dem hier beschriebenen Verfahren ist jedoch sicherzustellen, dass auch pseudonymisierte Meldungen nicht an einen beliebig großen Empfängerkreis gegeben werden dürfen. Die Erfahrung der letzten Jahre in der Anwendung des IFG hat gezeigt, dass nur eine normenklare und eindeutige Bestimmung einen hinreichenden Schutz von Betriebs- und Geschäftsgeheimnissen und eine interessengerechte Abwägung ermöglicht. Es ist mithin geboten, im Sinne der Rechtsklarheit und Rechtssicherheit sowohl für die verpflichteten Behörden als auch für die betroffenen Unternehmen eine Regelung zu finden, die nicht zu einer unverhältnismäßigen Ausweitung der Informationsweitergabe führen könnte. Dabei ist insbesondere zu bedenken, dass eine nicht hinreichend normenklare Regelung dem Schutzzweck des vorliegenden Gesetzentwurfs zuwider laufen kann, wenn hierdurch der Schutz der Betroffenen vor Angriffen in Frage gestellt wird. Hierbei ist auch zu bedenken, dass bereits weitgehende Meldepflichten auch gegenüber den Betroffenen im Falle des Datenabflusses nach Bundesdatenschutzgesetz (BDSG) bestehen.

Sollte es zu einer Herausgabe von Informationen gekommen sein, sind die Betroffenen unverzüglich darüber zu informieren. Eine dementsprechende Ergänzung muss in den Gesetzestext aufgenommen werden.

## 3. Kommentierung der Stellungnahme des Bundesrates 643/14

Im Folgenden wird auf die für die Versicherungswirtschaft wesentlichen Punkte aus der oben genannten Stellungnahme eingegangen.

Der Bundesrat begrüßt die Initiative der Bundesregierung und regt vor allem an, mehr Planungs- und Rechtssicherheit durch die Konkretisierung des Begriffs "erheblichen Störung" in § 8b Abs. 4 Satz 1 BSIG zu erreichen. Dieser Konkretisierungswunsch wird auch vom Verband geteilt und wurde bereits durch die Stellungnahme vom 9. Januar 2015 eingebracht.

### 3.1. Zu Nr. 5 der Stellungnahme

Weiterhin soll gemäß Nr. 5 der Stellungnahme in § 8b Abs. II Nr. 4c BSIG die Wörter "die zur Erfüllung ihrer Aufgaben erforderlichen" gestrichen und ans Ende (nach der Angabe "3") angefügt werden: ", insbesondere über Inhalte und Absender von Meldungen nach Absatz 4 mit möglichen Auswirkungen auf das jeweilig Land,".

Diese vorgeschlagene Streichung widerspricht der Gesetzeslogik. Eine Informationspflicht gegenüber den zuständigen Aufsichtsbehörden der Länder kann nicht über das hinausgehen, was zur Erfüllung ihrer Aufgaben zwingend notwendig ist. Hier gelten die gleichen strengen Maßstäbe wie für Bundesbehörden.

Zudem widerspricht die angeregte Ergänzung - und insbesondere die Nennung von Absendern - § 8b Abs. IV BSIG, wonach die Nennung der betroffenen Unternehmen eben nur erforderlich ist, „wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.“ Dies ist daher schon aus systematischen Gründen abzulehnen.

### 3.2. Zu Nr. 7 der Stellungnahme

Laut Nr. 7 zu § 10 Abs. 1 Satz 1 BSIG soll das Wort "Wirtschaftsverbände" durch das Wort "Branchenverbände" ersetzt werden.

Eine konsequente Terminologie im Gesetzentwurf wird befürwortet. Unabhängig davon muss klar gestellt werden, dass nur die Verbände an dem Verfahren zur Schaffung der Rechtsverordnung beteiligt sein dürfen, die auch das Mandat der jeweiligen Branche dafür mitbringen.

Berlin, den 26. Februar 2015