Deutsche Gesellschaft für Recht und Informatik e.V.

DGRI e. V. • Emmy-Noether-Straße 17 • D-76131 Karlsruhe

Geschäftsführung
Veronika Fischer

Bundesministerium des Innern
Herrn Dr. Philipp Spauschus
11014 Berlin

Vorab per Mail: philipp.spauschus @bmi.bund.de

Karlsruhe, 24.03.2015

Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (BT-Drucks. 18/4096)
Ihr Zeichen: ITII1-17002/7#2
Hier: Stellungnahme der Deutschen Gesellschaft für Recht und Informatik e.V. (DGRI)

Sehr geehrter Herr Dr. Spauschus, sehr geehrte Damen und Herren,

die Deutsche Gesellschaft für Recht und Informatik e.V. (DGRI) bedankt sich für die im Rahmen der Verbändeanhörung gewährte Gelegenheit zur Stellungnahme zu obigem Gesetzentwurf.

I.

Die DGRI ist eine der in Deutschland führenden unabhängigen wissenschaftlichen Vereinigungen auf dem Gebiet des IT-Rechts. Sie befasst sich mit Fragen an der Schnittstelle zwischen Informatik einerseits sowie Recht und Wirtschaft andererseits und fördert die Zusammenarbeit von Lehre, Forschung, Gesetzgebung und Praxis in allen Fragen der Informationstechnik. Zu ihren Mitgliedern zählen Wissenschaftler und Praktiker sowohl aus dem Gebiet der Rechtswissenschaft als auch der Technik. Mit ihnen sucht die Gesellschaft den ständigen Austausch von Wissen, Erfahrungen und Meinungen. Die DGRI begleitet mittels von der Gesellschaft veröffentlichter Stellungnahmen

Gesetzgebungsvorhaben auf nationaler wie europäischer Ebene als neutrale Institution, die den Partikularinteressen einzelner Unternehmen oder Branchen nicht verpflichtet ist.

II.

Der „Fachausschuss Datenschutz" hat sich mit dem Regierungsentwurf zu oben genanntem Gesetz befasst. In ihrer Stellungnahme nimmt die Gesellschaft Art. 4 (Änderung des TMG-Gesetzes) und einige Aspekte des Art. 5 (TKG-Änderung) aus datenschutzrechtlicher Perspektive in den Blick.

Wir nehmen dazu wie folgt Stellung:

A. Stellungnahme zu Art. 4 des IT-SiG: Änderungen des TMG (Einfügung eines neuen Absatz 7 bei § 13 TMG)

Bei dem im Rahmen des IT-SiG geplanten neuen Absatz 7 zu § 13 TMG fallen eine Reihe von Unstimmigkeiten und Begriffsungenauigkeiten auf, die zu einem Widerspruch zu den bestehenden Regelungen sowohl im TMG wie auch BDSG führen. Zudem beinhaltet die Regelung keinen Mehrwert im Verhältnis zur bestehenden Rechtslage, diese wird vielmehr durch die entstehenden Widersprüche verschlechtert, welche zu Rechtsunsicherheit führen.

1. Vorab

Folgt man der herrschenden Meinung, gilt das TMG für die Bestands- und Nutzungsdaten, das BDSG für die Inhaltsdaten. Zugleich soll das BDSG dann, wenn im TMG zu den Bestands- und Nutzungsdaten keine spezifischen Regelungen enthalten sind, ergänzend gelten.

Für den hier relevanten Bereich der Datensicherheit heißt dies, dass § 9 BDSG und dessen Anlagen auch für den Umgang mit personenbezogenen Bestands- und Nutzungsdaten gilt.

§ 9 BDSG lautet wie folgt:

> *„Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind*

Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

Es ist also von „Maßnahmen" die Rede, die „erforderlich" sein müssen; Maßstab dabei sind die Vorgaben des BDSG, insbesondere die 8 Schutzziele in der Anlage zu § 9 BDSG. Zugleich wird die Erforderlichkeit näher konkretisiert, nämlich dahingehend, dass der Aufwand der zu treffenden Schutzmaßnahmen im Verhältnis zum Schutzzweck steht.

Es handelt sich dabei im Ergebnis um ein in der Datensicherheit bewährtes Herangehen.

2. Die Vorschläge/ Formulierungen im neuen § 13 Abs. 7 TMG / Detailbewertung dazu

a. *„Diensteanbieter"*

Es stellt sich die Frage, ob es sachgerecht ist, Vorschriften im Rahmen der Umsetzung des IT-Sicherheitsgesetzes, welches sich auf kritische Infrastrukturen bezieht, generell auf sämtliche Diensteanbieter auszudehnen.

b. *„... haben, sowie dies technisch möglich und wirtschaftlich zumutbar ist (...)"*

§ 13 Abs. 7 TMG stellt also die zu treffenden Vorkehrungen unter den Vorbehalt, dass sie „technisch möglich" sowie „wirtschaftlich zumutbar" sein sollen.

Die Vorgabe, dass nur technisch mögliche Vorkehrungen zu treffen sind, ist eine Selbstverständlichkeit, zumindest wenn man diese Formulierung absolut versteht.

Soweit dagegen gemeint sein sollte (was unklar bleibt), dass nur die im konkreten Einzelfall technisch möglichen Vorkehrungen zu treffen sind, würde eine solche Forderung die Schutzanforderungen sehr niedrig setzen: Denn was im Einzelfall bei einem Diensteanbieter noch technisch möglich ist oder nicht, hängt alleine von diesem ab: Bei Diensteanbietern, die mit einer modernen und erweiterbaren IT-Struktur und Software arbeiten, ist viel mehr technisch möglich als bei einem Diensteanbieter, der „Billigsoftware" auf niedrigstem Schutzlevel betreibt.

Derjenige Diensteanbieter, der also schon von sich aus versucht, durch moderne Technik IT-Gefährdungen zu vermeiden, würde schlechter gestellt werden: Da bei ihm technisch deutlich mehr möglich als bei dem anderen Diensteanbieter ist, müsste er höheren Aufwand treiben.

Ferner sollen nach S. 2 des neuen Abs. 7 die Vorkehrungen den Stand der Technik berücksichtigen. Damit wird noch unklarer, was die Formulierung „technisch möglich" bedeuten soll: Denn der Stand der Technik ist ein Stand, der möglich ist, sonst wäre er nicht Stand der Technik.

Insofern ist dann aber ohnehin der Stand der Technik der Maßstab, nicht der konkrete Einzelfall und die Frage, was in diesem möglich ist.

Dann aber ist der Zusatz „*technisch möglich*" unnötig und sollte gestrichen werden, um obige Unklarheiten und Unsicherheiten zu beseitigen.

Gleiches gilt für die Frage der „wirtschaftlichen Zumutbarkeit": Denn der Stand der Technik gibt das Schutzniveau vor und hat die Frage der wirtschaftlichen Zumutbarkeit nicht im Blick. Ganz im Gegenteil ist der Stand der Technik davon unabhängig, da eben eine technische Frage und Anforderung, keine wirtschaftliche.

Zudem kann die wirtschaftliche Zumutbarkeit kein Kriterium sein, da höchst subjektiv:

Denn ein Startup-Diensteanbieter, der sich z.B. gerade selbstständig macht und dem nur ein minimales Budget zur Verfügung steht, hat deutlich weniger finanzielle Mittel zur Verfügung als ein bereits etablierter oder großer Diensteanbieter, der Teil eines Konzerns ist. Warum aber sollen die Besucher des „kleinen" Diensteanbieters mit einem schlechteren Schutzniveau konfrontiert sein als die eines großen Dienstleisters?

Wenn es um die in der Gesetzesbegründung angesprochene Gefahr der Verbreitung von Schadsoftware über Diensteanbieter geht, kann also die finanzielle Zumutbarkeit im Einzelfall kein Kriterium sein. Ansonsten wäre die Folge, dass ein über einen finanziell klammen Diensteanbieter verbreitete Schadsoftware „weniger schlimm" ist als wenn genau dieselbe Schadsoftware von einem wirtschaftlich potenten Anbieter verbreitet würde.

Dem gesamten Ziel des Gesetzes käme man damit nicht nur nicht näher, es wäre konterkariert.

Das Schutzniveau kann und darf also nicht von der wirtschaftlichen Zumutbarkeit im Einzelfall anhängen. Zudem widerspricht es dem Maßstab des „Stands der Technik". Es sollte gestrichen und vielmehr auf den Ansatz in § 9 BDSG abgestellt werden: einer Schutzbedarf-Ausrichtung.

c. „im Rahmen ihrer jeweiligen Verantwortlichkeit"

Auch diese Regelunge ist unklar und wenig hilfreich: Welche Verantwortlichkeit ist gemeint? Eine zivilrechtliche? Die Regelung des § 13 TMG befindet sich aber im Datenschutzteil des TMG.

Zudem stellt das Datenschutzrecht generell auf die verantwortliche Stelle ab und zwar auf die für die Datenverarbeitung verantwortliche Stelle. Es handelt sich dabei eher um eine faktische Verantwortlichkeit. Es sollte daher auch im TMG bei diesem Ansatz bleiben (was umso mehr gilt, dass das der EU-Datenschutz diese sehr deutsche Unterteilung in BDSG und TMG nicht kennt):

Für diejenige Datenverarbeitung, für die der Diensteanbieter im Sinne des BDSG die „verantwortliche Stelle" ist, hat er für ausreichende Vorkehrungen zu sorgen.

Es ist also auf die Datenverarbeitung als Maßstab abzustellen, wer wofür noch verantwortlich ist. Da dies im Datenschutzrecht ohnehin gilt, kann also auch dieser Passus ersatzlos gestrichen werden.

d. „sicherzustellen"

Das BDSG formuliert, dass erforderliche Maßnahmen „zu gewährleisten" sind. Der Begriff „sicherstellen", klingt nach einer verschuldensunabhängigen Garantiehaftung und sollte daher vermieden werden.

e. „für geschäftsmäßig angebotene Telemedien"

Hier stellt sich die Frage, was mit geschäftsmäßig gemeint ist und warum darauf eine Beschränkung erfolgt.

Jeder Diensteanbieter muss schon jetzt über § 9 BDSG technische und organisatorische Maßnahmen treffen, unabhängig, ob „geschäftsmäßig" oder nicht. Die Neuregelung führt also zu einer Absenkung des Schutzniveaus.

Zudem: Wäre die Webseite eines gemeinnützigen Vereins noch „geschäftsmäßig"? Die Gesetzesbegründung lehnt dies ab. Einer politischen Partei? Der Kirche?

In allen Fällen muss sich ein Diensteanbieter aber um IT-Sicherheit kümmern, die vor allem für die Besucher der Webseite relevant ist: Für diese kann und darf es aber keinen Unterschied machen, ob der Diensteanbieter (noch) geschäftsmäßig handelt oder nicht.

Mit anderen Worten: Warum ist die Gefahr, dass ein „Idealverein" (so die Gesetzesbegründung als Beispiel) Schadsoftware über seine Webseite verbreitet, geringer? Warum sollen dessen Webseitenbesucher weniger geschützt werden?

Diese Beschränkung sollte gestrichen werden.

f. „technische und organisatorische Vorkehrungen"

Hier stellt sich die Frage, warum nicht der in § 9 BDSG verwendete Begriff der „Maßnahmen" übernommen wurde. Wo soll der Unterschied liegen? Wenn es keinen Unterschied gibt, wäre auf den Begriff der „Maßnahmen" abzustellen.

Vorkehrungen geht zudem in Richtung fester technischer Apparaturen, Maßnahmen kann viel mehr auch noch organisatorische Maßnahmen meinen, denen eine gleichrangige Bedeutung zukommt.

g. *„Kein unerlaubter Zugriff möglich"* auf die *„genutzten technischen Einrichtungen"*

Zunächst ist zu betonen, dass die Zugriffskontrolle schon fester Bestandteil der Anlage zu § 9 BDSG, dort Nr. 3 ist. Die Formulierung dort ist aber eine etwas andere:

> *„zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können,"*

Es sind aber bei genauer Betrachtung zwei unterschiedliche Aspekte und Schutzziele geregelt, die sich ergänzen, was zu begrüßen ist:

- Die Nr. 3 der Anlage zu § 9 BDSG stellt auf die betriebsinternen Mitarbeiter ab (*„die zur Benutzung eines Datenverarbeitungssystems Berechtigten"),* die nicht über ihre Berechtigungen hinaus auf Daten zugreifen dürfen.

- Die Neuregelung in Abs. 7 dagegen ist allgemeiner formuliert und erfasst jeden, der keine Erlaubnis zum Zugriff hat.

Unklar ist aber, was mit „technischer Einrichtung" gemeint ist. Der Begriff findet sich etwa in § 87 Abs. 1 Nr. 6 BetrVG und ist dort sehr weit gefasst. Das Datenschutzrecht dagegen kennt ihn nicht. Es bezieht sich vielmehr auf die „Datenverarbeitungssysteme", etc. Insofern sollten die Begriffe konsistent verwendet werden.

h. „gegen Verletzungen des Schutzes personenbezogener Daten“

Die Formulierung „Verletzung des Schutzes“ ist unklar. Zudem muss eine Verletzung nicht zwingend rechtswidrig sein.

Es erscheint besser, auf die Rechtswidrigkeit abzustellen, die sich immerhin aus den Datenschutzgesetzen ergibt, also etwa in die Richtung

> *„ gegen rechtswidrige Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten“*

i. *„gegen Störungen“*

Dem Datenschutzrecht ist es fremd, sich gegen Störungen abzusichern, soweit diese keinen Einfluss auf die Verarbeitung personenbezogener Daten haben. Aber auch dann ist die Regelungsmechanik eine andere (nämlich etwa dahingehend, dass Daten nicht unrichtig sein dürfen).

Es handelt sich zudem weniger um eine datenschutzrechtliche Pflicht, da Störungen bei Telemedien nicht zwingend etwas mit personenbezogenen Daten zu tun haben oder haben müssen.

Zudem müsste man diese Formulierung im Gesetzesvorschlag aufgrund ihres Orts im Datenschutzkapitel so auslegen, dass nur Störungen gemeint sein können, die sich auf die Erhebung oder Verwendung von personenbezogenen Daten beziehen. Dann stellt sich aber die Frage, warum eine solche Beschränkung erfolgt, da auch andere Bereiche eines Telemediendienstes ein IT-Sicherheitsrisiko darstellen können und gegen Störungen zu schützen sind.

Der Begriff „Störung“ ist zudem unglücklich, da nicht jede Störung negative Auswirkungen haben muss. So ist etwa ein langsamer Server beim Diensteanbieter, der Bestellungen in einem Webshop langsamer abarbeitet, eine „Störung“, wo aber soll die Gefahr für die IT-Sicherheit liegen?

Der Begriff Störungen ist also zu definieren und muss sich auf solche Einwirkungen auf die Systeme beziehen, die Auswirkungen auf die Erhebung oder Verwendung personenbezogener Daten (oder besser: aller Daten) haben. Zudem sollte die Absicherung vor Störungen nicht auf personenbezogene Daten beschränkt sein.

j. „Stand der Technik“

Diese Formulierung ist positiv und hat sich seit ihrer Einführung zum 01.09.2009 im Rahmen der Anlage zu § 9 BDSG bewährt. Damalige Befürchtungen, dass zu hohe Anforderungen die Folge seien, haben sich nicht bewahrheitet. Vielmehr stellt diese Formulierung im ohnehin schon sehr umfänglich mit unbestimmten Rechtsbegriffen arbeitenden Datenschutzrecht einen guten Kompromiss dar.

k. „als sicher anerkanntes Verschlüsselungsverfahren"

Es handelt sich nur um ein Beispiel, das durchaus hilfreich ist, aber zugleich etwa bei den „Störungen" an der Sache vorbei geht: Wie soll eine Verschlüsselung etwa gegen Stromausfall helfen? Als bloße Beispielsformulierung schadet sie aber nicht.

3. Übergreifende Bewertung

Bei genauer Betrachtung bedarf es der Neuregelung in Abs. 7 nicht, da § 9 BDSG samt Anlage bereits die gleichen Vorgaben gibt und zwar umfassender. Würde man im TMG den Abs. 7 aufnehmen, im BDSG aber keine Anpassungen vornehmen, wäre die Folge, dass bei Bestandsdaten vorrangig nur dieser neue Abs. 7 in § 13 TMG gilt, § 9 BDSG aber verdrängt wird. Im Ergebnis wären Daten nach dem TMG damit weniger technisch und organisatorisch geschützt als Inhaltsdaten nach dem BDSG, was nicht der Fall sein darf: Denn der Schutzbedarf ist kein anderer, zudem ist die Abgrenzung ohnehin oft unklar.

Soweit man aber dennoch unbedingt eine Regelung im TMG wünscht, sollte diese begrifflich sehr eng an die Regelungen im BDSG zur Datensicherheit, aber auch allgemein an die Formulierungen im Datenschutzrecht angelehnt werden, um nicht Rechtsunsicherheit entstehen zu lassen. Jedenfalls ist klarzustellen, wie das Verhältnis zu § 9 BDSG und Anlage ist.

B. Stellungnahme zu Art. 5 des IT-SiG: Änderungen des TKG (Zur Einfügung von § 109 Abs. 2, § 109a Abs. 4, 5 und § 149 Nr. 21a TKG)

§ 109 Abs. 2 TKG

Wie bereits oben zum TMG ausgeführt, stellt sich die Frage, ob Begrifflichkeiten wie „technische Vorkehrungen und sonstige Schutzmaßnahmen" sowie „erforderlicher technischer und wirtschaftlicher Aufwand" nicht an die Begrifflichkeiten des § 9 BDSG angepasst werden sollten („technische und organisatorische Maßnahmen" und „Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck"), wobei der „Schutzzweck" noch den Umstand der kritischen Infrastruktur berücksichtigen müsste.

§ 109 Abs. 5 TKG, § 149 Nr. 21a TKG

Wünschenswert wäre eine Kategorisierung von meldepflichtigen Vorfällen, zum einen um unnötigen Melde-/Dokumentationsaufwand zu vermeiden, zum anderen um Rechtssicherheit zu gewährleisten, da bei Nichtmeldung ein Bußgeld drohen kann.

Bedenklich ist insoweit, dass nach Abs. 5 Satz 2 generalisierend Störungen eingeschlossen werden, welche die „Verfügbarkeit" der Dienste beeinträchtigen können, ohne dass quantifiziert wird, ab wann eine kritische Einschränkung der Verfügbarkeit vorliegt.

Ferner soll eine Meldepflicht bereits dann bestehen, wenn Störungen zur beträchtlichen Sicherheitsverletzungen „führen können". Dies wird zur Folge haben, dass Unternehmen vorsorglich jegliche Störung melden, was kontraproduktiv sein kann und für die Zielerreichung nicht erforderlich ist. Ziel des Gesetzes ist es in erster Linie, dem BSI einen Überblick über Vorfälle zu liefern, um diese auszuwerten und Erkenntnisse daraus anderen Betreibern zur Verfügung zu stellen. Dies ist im Zeitpunkt, in dem nur der Verdachtsmoment besteht, noch nicht möglich. Um dennoch eine Gefahrenabwehr zu ermöglichen, könnte man eine Meldung von Verdachtsfällen auf „offensichtlich zu beeinträchtigenden Sicherheitsverletzungen führen können" begrenzen, um die Norm auf ein allenfalls angemessenes Maß zu reduzieren.

Ergänzungsvorschlag zu § 109 Abs. Abs. 5 TKG: nach Satz 7:

„Im Übrigen gilt § 42a Satz 6 des Bundesdatenschutzgesetzes entsprechend."

Entsprechend § 109a Abs. 1 S. 5 TKG sollte ein Verweis auf § 42a BDSG Satz 6 BDSG erfolgen, um sicherzustellen, dass Erkenntnisse aus den Meldungen nicht im Rahmen von Straf- oder Ordnungswidrigkeitenverfahren gegen den Dienstebetreiber oder seine Mitarbeiter verwendet werden. Andernfalls steht zu befürchten, dass bei der Meldung Zurückhaltung ausgeübt wird.

§ 109a TKG

§ 109a TKG führt eine Mitteilungspflicht gegenüber Nutzern ein, sofern Störungen von einem Datenverarbeitungssystem des Nutzers ausgehen und der Nutzer dem Diensteanbieter bereits bekannt ist. Auch hier sollte die Meldepflicht entsprechend dem Schutzzweck und dessen, was angemessen ist, eingeschränkt werden. Zum einen wäre klarzustellen, dass eine solche Meldung nicht zu erfolgen hat, wenn dies laufende Ermittlungen gefährdet.

Zum anderen stellt sich die Frage, ob dem Diensteanbieter Kosten dafür aufgebürdet werden können, dass er die Nutzer in der Nutzung ihrer IT-Systeme unterweist. Angemessen erscheint eine solche Benachrichtigung nur dann, wenn dies zur Beseitigung der Störung im Interesse der Allgemeinheit erforderlich ist.

München, den 17.03.2015

- an der Unterschrift gehindert -

Dr. Sibylle Gierschmann, LL.M.
Leiterin FA Datenschutz

Dr. Robert Selk, LL.M.
Leiter FA Datenschutz

Für ergänzende Erläuterungen steht Ihnen die Gesellschaft gerne zur Verfügung.

Mit freundlichen Grüßen

Veronika Fischer
Rechtsanwältin
Geschäftsführerin der DGRI