DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht

zum Referentenentwurf des Bundesministeriums des Innern und für Heimat

für den "Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)"

Stellungnahme Nr.: 37/2024 Berlin, im Mai 2024

Mitglieder des Ausschusses Informationsrecht

- Rechtsanwalt Prof. Niko Härting, Berlin (Vorsitzender)
- Rechtsanwalt Dr. Simon Assion, Frankfurt
- Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf (Berichterstatterin)
- Rechtsanwältin Isabell Conrad, München
- Rechtsanwalt Prof. Dr. Malte Grützmacher, LL.M., Hamburg (Berichterstatter)
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf
- Rechtsanwalt Dr. Helmut Redeker, Bonn
- Rechtsanwältin Dr. Kristina Schreiber, Köln
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwalt/Rechtsanwältin Nicole Narewski, Berlin

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt ca. 60.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

Der DAV ist bereits in seiner Stellungnahme 35/2024 gesondert auf die Regelungen zur Haftung und zu den Pflichten von Geschäftsleitern in § 38 BSIG-RefE eingegangen. Er nimmt nachfolgend ergänzend Stellung zu einigen weiteren Aspekten des Referentenentwurfs zur Umsetzung der NIS-2-Richtlinie.

Der DAV begrüßt die gründliche Umsetzung, regt jedoch an,

- Cloud-Anbieter deutlicher in die Pflicht zu nehmen, da ein Großteil der Kritis-relevanten Unternehmen diese Anbieter nutzt;

- Auslagerungsunternehmen entweder selbst in die Pflicht zu nehmen oder jedenfalls deren jeweiligen Auftraggeber zu verpflichten,

- Auslagerungsunternehmen nach dem Vorbild der datenschutzrechtlichen Auftragsverarbeitung zu Sicherheits- und Vorsorgemaßnahmen vertraglich zu verpflichten;

- den Vorrang der Bewältigung von Sicherheitsvorfällen vor Meldepflichten gesetzlich festzuschreiben.

- sich zu bemühen, im weiteren Fortgang des Gesetzgebungsverfahrens für eine verbesserte Übersichtlichkeit der neuen Regelungen Sorge zu tragen.

1. Anwendungsbereich

Der DAV begrüßt ausdrücklich die Ausweitung der bisherigen Regulierung auf weitergehende Branchen.

Zugleich gibt der DAV jedoch zu bedenken, dass der Gesetzesentwurf regelmäßig den Hersteller von IT-Systemen in den Fokus nimmt, nicht aber auf Anbieter von IT-Systemen im Übrigen, insbesondere auf Cloud-Anbieter abstellt. Nur vereinzelt – und sonst im Gegenschluss vielfach nicht – wird auch auf Diensteanbieter abgestellt (vgl. etwa § 55 oder § 57 BSIG-RefE). Nur TK-Provider sollen *niederschwellig* auch eine „besonders wichtige Einrichtung“ im Sinne von § 28 Abs. 1 Nr. 3 BSIG-RefE darstellen. Der DAV begrüßt aber, dass Cloud-Dienstleister und Rechenzentrumsdienstleister von § 28 Abs. 1 Nr. 4 i.V.m Anlage I, Ziff. 6.1.4 BSIG-RefE nunmehr (anders als in Vorentwürfen) immerhin auch als besonders wichtige Einrichtungen erfasst werden, wenn auch erst bei (i) mindestens 250 Mitarbeitern oder (ii) einem Jahresumsatz von über 50 Millionen Euro sowie einer Jahresbilanzsumme von über 43 Millionen Euro. Ob weiter die landesrechtlichen Vorschriften i.S.d. der Rückausnahme des § 28 Abs. 9 BSIG-RefE zu einer ausreichenden, vergleichbaren Regulierung führen, vermag der DAV nicht zu beurteilen; dieses sollte kritisch geprüft und ggf. geändert werden, damit die nun erfolgte Einbeziehung nicht hierdurch wieder rückgängig gemacht werden kann, indem bspw. entsprechende Kriterien definiert werden, wann eine solche Gegenausnahme nicht angezeigt ist, insb. in der Lieferkette (s.u. Ziff.2).

Cloud-Anbieter werden im Übrigen in § 2 Abs. 1 Nr. 3 BSIG-RefE definiert und nur in § 28 Abs. 9, § 30 Abs. 3 und § 64 Abs. 1 BSIG-RefE und Anlage 1, Ziff. 6.1.4 angesprochen. Dies obwohl Cloud-Anbieter bereits heute einen Großteil der Infrastruktur der Kritis-relevanten Unternehmen bereitstellen. Abzuwarten bleibt vor diesem Hintergrund, inwieweit Cloud-Anbieter und sonstige vergleichbare Provider als Betreiber kritischer Anlagen i.S.v. § 31 BSIG-RefE eingeordnet werden. Es darf bezweifelt werden, dass der Verordnungsgeber (vgl. § 28 Abs. 7, § 58 Abs. 4 BSIG-RefE) alle wesentlichen Cloud-Anbieter als Betreiber kritischer Anlagen einstufen werden wird. Auch stellen sich ggf. schwierige Fragen der Anwendbarkeit des

Rechts und der Zuständigkeit für solche Anbieter, die ihre Dienste aus dem EU-Ausland bzw. aus Drittstaaten heraus anbieten (vgl. dazu § 64 BSIG-RefE).

Die NIS-2-Richtlinie gibt lediglich eine Mindestharmonisierung und keine Vollharmonisierung vor. Daher ist zu erwägen, den Anwendungsbereich mit Blick auf Cloud-Anbieter weitergehend zu fassen und auch diese direkt zu regulieren, zumindest dann, wenn es sich um Anbieter einer gewissen Größe und/oder von einem gewissen Marktanteil handelt. Hiergegen mag eingewandt werden, dass diese Anbieter, soweit sie nicht besonders zentral sowie ihre Leistungen unumgänglich sind, selbst entscheiden können sollten, ob sie Kritis-relevante Leistungen anbieten wollen. Die IT-Leistungen von marktführenden Cloud-Anbietern sind indes per se Kritis-relevant, da fundamental für das Funktionieren der deutschen Wirtschaft. Dies gilt umso mehr, als der personelle Anwendungsbereich des BSIG in Umsetzung der NIS-2-Richtlinie erheblich ausgedehnt werden wird.

2. Auslagerung

Unabhängig davon, ob man in territorialer oder sachlicher Hinsicht eine weitgehende direkte Regulierung für erforderlich hält oder nicht, sollte zumindest in denjenigen Fällen, in denen Auslagerungsunternehmen (etwa Cloud-, Outsourcing-, Rechenzentrums- oder sonstige Provider) ihre IT-Leistung Kritis-relevanten Unternehmen zur Verfügung stellen, eine Regulierung dieser Auslagerung derart erfolgen, dass das Gesetz vorschreibt, dass auch das Auslagerungsunternehmen vertraglich (gewissermaßen anstelle des Kritis-Unternehmens) gewisse Rechte und Pflichten übernimmt. Dieses Prinzip ist seit langem in vergleichbar regulierten Bereichen des IT-Rechts anerkannt. Es wurde etwa schon in § 11 BDSG a.F. vorgesehen sowie sodann in Artikel 28 DSGVO. Weiterhin ist es bekannt aus dem Versicherungs- sowie Bankrecht, nämlich aus § 32 VAG sowie aus § 25b Abs. 3 S. 3 KWG. Es ist zu bezweifeln, dass dieses allein durch die Anforderungen an die zu ergreifenden Maßnahmen nach § 30 Abs 2 S. 2 Nr. 4 BSIG-RefE ("*Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern*") bzw. die der Parallelnormen in § 5c Abs. 3 S. Nr. 4 EnWG-RefE oder § 165 Abs. 2 aNr. 4 TKG-RefE gewährleistet ist. Dabei ist zu berücksichtigen,

dass lediglich allgemeine Maßnahmen nach dem Stand der Technik vorgesehen sind, ohne jedoch wie in den hier zuvor angeführten Fällen auf den konkreten Gegenstand der Auslagerung und dessen spezifische Risiken abzustellen, das jeweilige back-to-back Risiko abzusichern und hierfür gegenüber dem Auftraggeber in der Regresskette vertraglich verantwortlich zu sein.

Hierzu ist im Detail Folgendes anzumerken:

- Sinnvoll erscheint es, das Auslagerungsunternehmen selbst als Auftragnehmer (im Datenschutzrecht Auftragsverarbeiter) direkt in die Pflicht zu nehmen, wie dieses in Artikel 28 DSGVO vorgesehen ist. Mindestens aber sollte im Gesetz – wie einst im Datenschutzrecht in § 11 Abs. 1 S. 1 BDSG a.F. – geregelt werden, dass das Kritis-Unternehmen eine Auslagerung nur dann vornehmen darf, wenn bestimmte Pflichten im Vertrag verankert werden. Während im ersten Fall (vgl. Artikel 28 DSGVO) auch das Auslagerungsunternehmen selbst direkte Pflichten trifft und insofern Normadressat und somit ggf. auch Adressat von bußgeldbewährten Bestimmungen wird, wäre im letztgenannten Fall (§ 11 BDSG a.F.) nur eine mittelbare Verpflichtung vorzusehen, derzufolge sich das Kritis-relevante Unternehmen pflichtwidrig verhielte und ggf. Bußgeldern ausgesetzt sähe, würde es bestimmte gesetzliche Pflichten, die es selbst trifft, nicht an das Auslagerungsunternehmen weiterreichen.

- Eine solche Regulierung ist aus Sicht des DAV erforderlich, weil die Praxis zeigt, dass Kritis-relevante Unternehmen sich bislang äußerst schwertun, die sie treffenden Normen vertraglich (back-to-back) an das Auslagerungsunternehmen durchzureichen. In Vertragsverhandlungen ist oft umstritten, inwieweit eine Weiterverlagerung der Pflichten auf diese Unternehmen erforderlich ist. Auslagerungsunternehmen wenden gerne ein, sie seien selbst ja nicht reguliert und deshalb entsprechenden Pflichten nicht unterworfen. Mag Letzteres zutreffend sein, ist Ersteres mehr als zweifelhaft. So vertritt auch das BSI, insbesondere zu § 8a BSI-Gesetz, die Auffassung, dass das Kritis-relevante-Unternehmen im Auslagerungsfall weiterhin vollumfänglich in der Pflicht steht und deshalb gehalten ist, entsprechende

Regelungen back-to-back zu vereinbaren. Gerade Anbietern aus anderen Rechtsordnungen/-kreisen ist diese Rechtsauffassung allerdings nicht immer leicht zu vermitteln, so dass letztlich ein ganz erhebliches Risiko der Nicht-Compliance auf Seiten des Kritis-relevanten Unternehmens verbleibt, wenn der Gesetzgeber keine stützenden Regelungen vornimmt. Und würde man sich andersherum mit den entsprechenden Providern auf den Standpunkt stellen, dass diese auch nicht nötig wären, so hieße dieses im Ergebnis, dass Kritis-relevante Unternehmen ihren gesetzlichen Pflichten entkommen könnten, indem sie ihre IT auf Dritte auslagern. Dies liegt nicht im Interesse der IT-Sicherheit und damit der nationalen Versorgungssicherheit. Eine gesetzgeberische Klarstellung würde der Informationssicherheit im Markt erheblichen Rückhalt geben und eine verbesserte Rechtssicherheit bringen.

Im Ergebnis erscheint es zwingend, Regelungen analog Artikel 28 DSGVO (bzw. § 11 BDSG a.F.) vorzusehen und zumindest für einen Mindestkanon von Pflichten festzuschreiben, dass diese auch vertraglich gegenüber dem Auslagerungsunternehmen vertraglich vereinbart werden müssen. Hierzu sollten gehören:

- Die Pflicht, technische und organisatorische Maßnahmen nach dem Stand der Technik vorzusehen, sollte vertraglich zu vereinbaren sein.

- § 30 Abs 2 S. 2 Nr. 4 BSIG-RefE bzw. die Parallelnormen in § 5c Abs. 3 S. Nr. 4 EnWG-RefE und § 165 Abs. 2 aNr. 4 TKG-RefE mag man in diese Richtung deuten; sie sind aber nicht deutlich genug formuliert.

- Auslagerungsunternehmen sollten weiterhin vertraglich verpflichtet werden, die IT-Sicherheit bzw. Compliance mit Blick auf technische und organisatorische Maßnahmen durch entsprechende Zertifikate oder sonstige Dokumentationen (vgl. § 39 BSIG-RefE) auf Verlangen des Kritis-relevanten Unternehmens nachzuweisen.

- Auslagerungsunternehmen sollten, ähnlich wie auch im Datenschutzrecht, vertraglich angehalten werden, bei Prüfungen und Audits durch die

Aufsichtsbehörden mitzuwirken und den Auftraggeber zu unterstützen sowie die hierfür erforderlichen Nachweise zur Verfügung zu stellen.

- Die Auslagerungsunternehmen sollten analog der Meldepflicht des Auftraggebers ihrerseits gehalten sein, Meldungen i.S.v. § 32 BSIG-RefE entweder an den Auftraggeber oder an das BSI direkt vorzunehmen und den Auftraggeber bei der Meldung zu unterstützen. Insofern besteht eine Parallelität zu Artikel 33 DSGVO und der Regelung in Artikel 28 Abs. 3 Satz 2 lit. f DSGVO.

- Auslagerungsunternehmen sollten bei weiterer Unterbeauftragung verpflichtet werden, diese Pflichten mit Prüfrechten des Auftraggebers an ihren Unterauftragnehmer wie nach Art. 28 Abs. 4 DSGVO weiterzugeben. Zudem sollten Sie wie nach Art. 28 Abs. 4 S. 2 DSGVO dem Auftraggeber gegenüber haften, wenn der weitere Unterauftragnehmer seinen Pflichten nicht nachkommt. Weiterhin sollte festgelegt werden, ob und wenn in welchen Fällen eine solche weitere Unterbeauftragung ausgeschlossen sein sollte.

3. Vorrang der Bewältigung von Sicherheitsvorfällen

Der DAV regt an, die Regelungen der in § 32 BSIG-RefE statuierten Meldepflichten dahingehend zu ergänzen, dass die Bewältigung des erheblichen Sicherheitsvorfalls vorrangig vor der Meldepflicht ist. Nach Erwägungsgrund 102 der NIS-2-Richtlinie sollen die Mitgliedstaaten sicherstellen, dass die Erfüllung der Meldepflichten nicht dazu führt, dass die meldende Einrichtung die Ressourcen von Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen umlenken müssen. Auch wenn eine entsprechende Regelung durch die Richtlinie nicht zwingend vorgeschrieben ist, sollte der deutsche Gesetzgeber beachten, dass gerade unmittelbar nach der Kenntniserlangung eines erheblichen Sicherheitsvorfalls die der Einrichtung zur Verfügung stehenden personellen Kapazitäten begrenzt sind.

4. Übersichtlichkeit

Der DAV regt abschließend an, zu prüfen, ob sich das Gesetz nicht kürzer fassen lässt, indem redundante Regelungen gestrichen werden und der Entwurf sich näher an den Richtlinientext anlehnt.

Der Gesetzesentwurf enthält eine so große Vielzahl von Normen, dass der Ausschuss sich fragt, ob dies der Rechtsanwendung förderlich ist. Der Entwurf ist zudem durch verschiedene, sich offenbar überschneidende Begriffsebenen sowie zahlreiche Querverweise gekennzeichnet und daher nur sehr schwer zu durchdringen. Auch dies ist der Rechtsanwendung nicht förderlich.

Verteiler

Deutschland

Bundesministerium des Innern und für Heimat
Bundesministerium der Justiz
Bundesministerium für Wirtschaft und Klimaschutz

Ausschuss für Inneres und Heimat im Deutschen Bundestag
Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitales im Deutschen Bundestag
Fraktionen im Deutschen Bundestag

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Die Justizministerien der Länder
Die Datenschutzbeauftragten der Bundesländer

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe e.V.
Deutscher Richterbund, Bund der Richterinnen und Richter, Staatsanwältinnen und
Bund Deutscher Verwaltungsrichter und Verwaltungsrichterinnen
Staatsanwälte e.V. (DRB)
Deutscher Notarverein
Deutscher Steuerberaterverband e.V. Berlin
Bundesverband der Deutschen Industrie e.V.
Arbeitsgemeinschaft berufsständischer Versorgungseinrichtungen e.V.
Deutscher EDV-Gerichtstag e.V.
GRUR - Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht e.V.
Bitkom e. V.
Deutsche Gesellschaft für Recht und Informatik e.V. (DGRI)
ver.di - Vereinte Dienstleistungsgewerkschaft
Gewerkschaft der Polizei
Deutsche Polizeigewerkschaft im DBB (DPolG)

DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungsausschüsse
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Presse

Frankfurter Allgemeine Zeitung GmbH
Süddeutsche Zeitung GmbH
Redaktion NJW
JUVE Verlag für juristische Information GmbH

Redaktion Legal Tribune Online / LTO
Redaktion Anwaltsblatt
juris GmbH
Redaktion MultiMedia und Recht (MMR)
Redaktion Zeitschrift für Datenschutz ZD
Redaktion heise online
DER SPIEGEL GmbH & Co. KG