Stellungnahme

zum Entwurf des Umsetzungskonzepts Cybersicherheit (§§ 9, 9a LuftSiG)

DSLV Bundesverband Spedition und Logistik e. V.

Friedrichstraße 155-156 | Unter den Linden 24
10117 Berlin

Telefon: +49 30 4050228-0
E-Mail: info@dslv.spediteure.de
www.dslv.org | de.linkedin.com/company/spediteure

Lobbyregister beim Deutschen Bundestag | Registernummer: R000415
Transparenz-Register der EU | Identifikationsnummer: 7455137131-52

Stand: 15. September 2023

Zum Entwurf der

Grundsätze zur Umsetzung der DVO (EU) 2019/1583 der Kommission vom 25. September 2019 zur Änderung der Verordnung (EU) 2015/1998 zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit in Bezug auf Cybersicherheitsmaßnahmen

im Zuständigkeitsbereich des Bundesministeriums für Digitales und Verkehr (§§ 9 und 9a LuftSiG) nimmt der DSLV wie folgt Stellung:

Grundsätzliche Erwägungen

Notwendige Harmonisierung mit gesonderten Cybersicherheitsanforderungen

Sollten Luftfahrtunternehmen und Stellen gesonderten Cybersicherheitsanforderungen unterliegen, die sich aus anderen EU- oder nationalen Rechtsvorschriften ergeben, kann nach Nr. 1.7.5. des Anhangs der DVO (EU) 2015/1998 die zuständige Behörde entscheiden, dass die Einhaltung der Cyber-Anforderungen dieser Verordnung durch die Einhaltung der Elemente anderer EU- oder nationaler Rechtsvorschriften ersetzt wird. Weiterhin sollen u. a. Maßnahmen, die auf der NIS-Richtlinie (und der zukünftigen NIS2-Richtlinie) und der DVO (EU) 2015/1998 basieren, auf nationaler Ebene koordiniert werden, um Lücken oder eine doppelte Übertragung von Verpflichtungen zu vermeiden.

Dieser Aspekt sollte auch im Umsetzungskonzept expressis verbis aufgegriffen und festgeschrieben werden. Dies betrifft u. a. die Registrierungs- und Meldepflicht unter Nummer 8 des Entwurfs. Um unnötige Doppelungen zu vermeiden, sollte für Unternehmen, die auch der Registrierungspflicht der NIS2 unterliegen, eine einzige Registrierung ausreichen.

Wir erinnern in diesem Zusammenhang auch an die Aussage im Verbändegespräch Luftsicherheit am 17. Mai 2023, vorhandene Qualifizierungen, wie z. B. eine Zertifizierung nach der internationalen Norm ISO/IEC 27001, anzuerkennen. Diese Norm spezifiziert die Anforderungen für Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-Managementsystems und beinhaltet Anforderungen für die Beurteilung und Behandlung von Informationssicherheitsrisiken. Die Anerkennung einer Zertifizierung nach ISO/IEC 27001 sollte im Umsetzungskonzept festgeschrieben werden.

Ausweitung der Umsetzungsfrist

Aus unserer Sicht bleibt unklar, wie die betroffenen Unternehmen zeitnah eine europäisch und national rechtskonforme Erfüllung der Anforderungen sicherstellen können, da es erhebliche Verzögerungen bei der Formulierung der nationalen Umsetzungsgrundsätze gab.

Diese liegen jetzt erst in der Entwurfsfassung vor; Rückmeldungen der Mitgliedsbetriebe zeigen, dass weitere Präzisierungen erforderlich sind. Gemäß Nummer 7 des Entwurfs haben Unternehmen die Möglichkeit, die erforderlichen Informationen bezüglich Cybersicherheit erst mit der „nächsten notwendigen Änderung oder spätestens der Überarbeitung im Zuge der wiederholenden Zulassung“ einzureichen. Dadurch ergibt sich nur ein geringfügig längerer Zeitraum für die Umsetzung. Dass der Gesetzgeber die angekündigten Umsetzungsgrundsätze nicht rechtzeitig vorgelegt hat, hat zu Rechtsunsicherheit bei den betroffenen Unternehmen geführt. Dieser Verzug darf nicht zu Lasten der Stellen gehen. Wir plädieren ausdrücklich dafür, einen angemessenen Übergangszeitraum festzulegen und die Verzögerungen gegebenenfalls bei der Europäischen Kommission anzuzeigen.

Mündliche Erörterung

Aufgrund der Komplexität der Grundsätze regen wir an, uns Gelegenheit zu einer mündlichen Erörterung einzuräumen.

Zu Nummer 4 - Ermittlung kritischer informations- und kommunikationstechnischer Systeme und Daten nach Nr. 1.7.1. des Anhangs der DVO (EU) 2015/1998

„Dabei sind auch Systeme und Daten zu betrachten, die im Auftrag der Luftfahrtunternehmen und der Stellen von Dritten betrieben werden (z. B. Handlingsagenten).“

Es wäre zu präzisieren, was diese Anforderung im Einzelnen beinhalten soll und wie sie praktisch umsetzbar ist. Selbst im Fall eines Auftragsverhältnisses handelt es sich bei Dritten um rechtlich selbstständige Unternehmen, die nicht ohne Weiteres Einblick in ihre Systeme und Daten gewähren. Die Anforderungen dürften die Beteiligten der sicheren Lieferkette jedenfalls vor hohe Schwierigkeiten stellen, wenn die Erfüllung nicht sogar unmöglich ist.

Zu Nummer 7 - Zulassung des Sicherheitsprogramms durch die zuständige Luftsicherheitsbehörde

Zulassung des Sicherheitsprogramms und Sprachfassung von Anlagen

Informationen bzw. Anlagen in Bezug auf Cybersicherheitsmaßnahmen liegen bei international tätigen Unternehmen primär in englischer Sprache vor. Englisch ist die relevante Arbeitssprache in dem Fachbereich. Wir vermissen daher eine Regelung, dass Anlagen zum Sicherheitsprogramm auch in englischer Sprache verfasst sein können. In Einklang mit den geltenden Bestimmungen aus dem Verwaltungsverfahrensgesetz (VwVfG) und um unnötige und kostspielige Übersetzungsleistungen zu vermeiden, sollte die Option in den Entwurf

aufgenommen werden, die erforderlichen Anlagen vollständig oder teilweise in englischer Sprache einreichen zu dürfen.

Zuweisung der neuen Verantwortlichkeiten für Administratoren

Auf Basis des Entwurfs bleibt unklar, welche rechtlich verpflichtende Zuweisung der Verantwortlichkeit für die Administratoren (Personen mit Administrationsrechten zur Änderung der KIKS) sich letztendlich ergibt. Administratoren können im Rahmen ihrer Tätigkeit mehrere zugelassene Standorte betreuen. Sie sind nicht eindeutig einem Betriebsstandort zuzuordnen. Daraus ergibt sich die Frage, ob eine Zuordnung aller relevanten Administratoren für jeden Betriebsstandort einzeln und separat erfolgen muss. Je nach Anzahl der Standorte wäre dies mit enormen bürokratischen und administrativen Aufwänden verbunden. Eine Regelung, die es ermöglicht, dass beispielsweise der zentrale Luftfrachtsicherheitsbeauftragte einer Stelle die notwendigen Informationen wie ZÜP-Nachweise vorhalten darf, würde helfen. Wir bitten, dies zu prüfen bzw. Klarheit zu schaffen.

Zu Nummer 8 - Melde- und Informationswesen; Vorfallbehandlung

Benennung der Kontaktstelle

Der Entwurf fordert von Luftfahrtunternehmen und Stellen die Registrierung und Benennung einer Kontaktstelle, über die sie jederzeit erreichbar sind. Wir weisen darauf hin, dass international tätige Unternehmen üblicherweise über eine zentralisierte Struktur für Cybersicherheit verfügen und das zuständige Personal in der Regel nicht in allen Ländern bzw. an allen Betriebsstandorten ansässig ist. Lokale IT-Verantwortliche hätten im Falle eines relevanten Cybervorfalls keinen oder nur sehr geringen Einfluss. Es sollte daher klargestellt werden, dass Unternehmen, die mehrere Standorte betreiben, eine zentrale Kontaktstelle für alle Anfragen zur Cybersicherheit benennen dürfen. Dies könnten z. B. die Kontakte / E-Mailadressen des zuständigen Cybersicherheits-Teams sein.

Zu Nummer 9 – Zuverlässigkeitsüberprüfungen

ZÜP für im Ausland ansässige Personen mit Administrationsrechten

Danach müssen Personen, die unbeaufsichtigt und unbeschränkt Zugang zu diesen Systemen haben, sowie Personen mit Administrationsrechten einer ZÜP in Deutschland unterzogen werden, unabhängig davon, ob sie sich bereits in Deutschland aufgehalten haben oder nicht. Es kommt jedoch häufig vor, dass Unternehmen ihre IT-Dienstleistungen an Softwareunternehmen außerhalb der EU auslagern. Die Anforderung, für solche Personen mit Wohnsitz im Ausland eine ZÜP durchzuführen, ist unzweckmäßig und praktisch nicht zu erfüllen. Nur die

Landesluftsicherheitsbehörde kann in Deutschland eine erweiterte ZÜP durchführen. Eine Anerkennung einer gleichwertigen europäischen oder drittstaatlichen Überprüfung der Zuverlässigkeit durch den Gesetzgeber ist bislang nicht möglich.

Aus unserer Sicht muss grundlegend geklärt werden, wie die Zuverlässigkeit von im Ausland ansässigen Personengruppen in Deutschland bestätigt werden kann. Dabei sollte auch die gegenseitige Anerkennung von Zuverlässigkeitsüberprüfungen zwischen den EU-Mitgliedstaaten, aber auch von Staaten mit als gleichwertig anerkannten Sicherheitsstandards (wie z. B. den USA oder dem Vereinigten Königreich), geprüft werden.

Zu umfassende Protokollierungspflicht

Laut Nummer 9 des Entwurfs müssen alle Zugriffe und Tätigkeiten protokolliert werden. Im Anschluss hat eine Überprüfung der Protokolldaten zu erfolgen, die zu dokumentieren ist. Diese Anforderung ist zu umfassend, ohne dass ein Sicherheitsgewinn erzeugt wird. Alternativ sollte ein risikobasierter und datensparender Ansatz gewählt werden, so dass die Protokollpflicht nur auf begründete Risikobereiche und/oder Personenkreise reduziert wird.

Zu Nummer 10 - Eignung und Schulung nach Nr. 11.2.8. des Anhangs der DVO (EU) 2015/1998

Ausufernde Schulungsumfänge

Der Entwurf geht deutlich über die europäischen Vorgaben für die zu schulenden Personen hinaus. Nach Nr. 11.2.8 sind „Personen mit Funktionen und Verantwortlichkeiten in Bezug auf Cyberbedrohungen“ zu schulen. Darunter fallen potenziell Personen, die Zugang zu kritischen Daten oder Systemen haben. „Personengruppe a“ hingegen definiert eine Gruppe, die in keinem sachlichen oder praktischen Zusammenhang zu möglichen Verantwortlichkeiten in Bezug auf Cyberbedrohungen steht und auch keinen Zugang hat. Eine jährliche Sensibilisierung in Bezug auf Cybersecurity scheint uns deshalb nicht geboten. Die Personengruppe a sollte daher von Schulungsanforderungen ausgenommen werden.

Grundlegend sollte die gegenseitige Anerkennung von Schulungen zwischen den EU-Mitgliedstaaten, sowie von Staaten mit als gleichwertig anerkannten Sicherheitsstandards, auch im Hinblick auf Cybersicherheit, bestätigt bzw. geprüft werden.

Verbandsstruktur, Leistungsprofil und Leitlinien

Als Spitzen- und Bundesverband repräsentiert der DSLV durch 16 regionale Landesverbände die verkehrsträgerübergreifenden Interessen der 3.000 führenden deutschen Speditions- und Logistikbetriebe, die mit insgesamt 600.000 Beschäftigten und einem jährlichen Branchenumsatz in Höhe von 135 Milliarden Euro wesentlicher Teil der drittgrößten Branche Deutschlands sind (Stand: Juli 2022).

Die Mitgliederstruktur des DSLV reicht von global agierenden Logistikkonzernen, 4PL- und 3PL-Providern über inhabergeführte Speditionshäuser (KMU) mit eigenen LKW-Flotten sowie Befrachter von Binnenschiffen und Eisenbahnen bis hin zu See-, Luftfracht-, Zoll- und Lagerspezialisten.

Speditionen fördern und stärken die funktionale Verknüpfung sämtlicher Verkehrsträger. Die Verbandspolitik des DSLV wird deshalb maßgeblich durch die verkehrsträgerübergreifende Organisations- und Steuerungsfunktion des Spediteurs bestimmt.

Der DSLV ist politisches Sprachrohr sowie zentraler Ansprechpartner für die Bundesregierung, für die Institutionen von Bundestag und Bundesrat sowie für alle relevanten Bundesministerien und -behörden im Gesetzgebungs- und Gesetzumsetzungsprozess, soweit die Logistik und die Güterbeförderung betroffen sind.

Gemeinsam mit seinen Landesverbänden ist der DSLV Berater und Dienstleister für die Unternehmen seiner Branche. Als Arbeitgeberverbände und Sozialpartner vertreten die DSLV-Landesverbände die Branche in regionalen Tarifangelegenheiten.

Der DSLV ist Mitglied des Europäischen Verbands für Spedition, Transport, Logistik und Zolldienstleistung (CLECAT), Brüssel, der Internationalen Föderation der Spediteurorganisationen (FIATA), Genf, sowie assoziiertes Mitglied der Internationalen Straßentransport-Union (IRU), Genf. In diesen internationalen Netzwerken nimmt der DSLV auch Einfluss auf die Entwicklung des EU-Rechts in Brüssel und Straßburg und auf internationale Übereinkommen der UN, der WTO, der WCO, u. a.

Die Mitgliedsunternehmen des DSLV fühlen sich den Zielen der Sozialen Marktwirtschaft und der Europäischen Union verpflichtet.