Stellungnahme

zum Referentenentwurf des Bundesministeriums des Innern für eine Nationale Luftsicherheitsprogramm-Verordnung (NLspV)

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: 18. November 2025

Zum Referentenentwurf des Bundesministeriums des Innern für eine Nationale Luftsicherheitsprogramm-Verordnung (NLspV) nimmt der DSLV Bundesverband Spedition und Logistik e. V. wie folgt Stellung:

Die Luftsicherheit ist für den DSLV und seine Mitgliedsunternehmen von höchster Priorität. Die deutschen Speditions- und Logistikunternehmen agieren bereits heute nach höchsten Sicherheitsstandards, investieren erheblich in Compliance-Strukturen und verfügen über etablierte Sicherheitsprogramme.

Der DSLV setzt sich für eine praxistaugliche, rechtssichere und ressourceneffiziente Umsetzung der europäischen Luftsicherheitsvorgaben ein. Bürokratische Doppelstrukturen, unverhältnismäßige administrative Lasten und redundante Genehmigungsverfahren gefährden die Wettbewerbsfähigkeit deutscher Unternehmen und müssen vermieden werden. Die bereits hohen Standortbelastungen durch Gebührenverordnung (9. LuftSiGebV) und regulatorische Anforderungen erfordern ein Höchstmaß an Effizienzorientierung bei neuen Regelungen.

Die Formulierung der NLspV sollte zudem auf direkte inhaltliche Bezüge zu einzelnen EU-Durchführungsverordnungen verzichten. Bei Aktualisierung oder Ersetzung einer EU-VO könnten nationale Verordnungen mit direkten Bezügen ungültig oder missverständlich werden. Allgemeine Formulierungen gewährleisten die Zukunftssicherheit der deutschen Regelung, während das LBA stets auf Basis der aktuell gültigen EU-Durchführungsverordnung arbeiten kann.

Zu § 20 Abs. 1 – Sicherheitsbeauftragter

Entwurfstext:
„Ein Sicherheitsbeauftragter eines Beteiligten an der sicheren Lieferkette [...] darf nicht gleichzeitig als Sicherheitsbeauftragter eines weiteren Betriebsstandortes oder eines anderen Beteiligten an der sicheren Lieferkette benannt sein."

Position des DSLV

Der Absatz ist dahingehend zu präzisieren, dass stellvertretende Sicherheitsbeauftragte von diesem Verbot ausgenommen sind.

Es ist gelebte Praxis, dass eine Person als Sicherheitsbeauftragter für einen Betriebsstandort bestellt ist und gleichzeitig als stellvertretender Sicherheitsbeauftragter (z. B. zeitlich begrenzte Urlaubsvertretung) für einen weiteren Betriebsstandort fungiert. Diese Praxis ist wirtschaftlich notwendig und belastet Unternehmen nicht unverhältnismäßig.

§ 20 Abs. 1 sollte wie folgt ergänzt werden: „Die Benennung als stellvertretender Sicherheitsbeauftragter für einen weiteren Betriebsstandort bleibt hiervon unberührt, insbesondere für zeitlich begrenzte Vertretungen."

Zu § 22 – Informationssicherheitsmaßnahmen der Beteiligten an der sicheren Lieferkette
Zu Anlage 2 Abschnitt 2 – Definition kritischer informations- und kommunikationstechnischer Systeme (KIKS)

Entwurfstext (Anlage 2 Abschnitt 1, Ziffer 1.1.2):
„Kritische informations- und kommunikationstechnische Systeme und Daten sind alle Systeme und Daten, welche bei Einschränkung ihrer Vertraulichkeit, Integrität oder Verfügbarkeit das Sicherheitsniveau der Zivilluftfahrt absenken können. [...] Zusätzlich gehören dazu analoge Daten, die im Zusammenhang mit Luftsicherheitsmaßnahmen gelagert, verarbeitet, eingesehen oder transportiert werden."

Position des DSLV

1. Analoge Daten sind keine KIKS

Die Einordnung analoger Daten als KIKS ist nicht sachgerecht. Analoge Daten (Unterlagen in Papierform) sind keine informations- und kommunikationstechnischen Systeme. Der Schutz von Unterlagen in Papierform wird bereits durch die bestehenden Sicherheitsprogramme und Schulungen gewährleistet.

Obwohl Informationssicherheitsexperten anerkennen, dass Informationssicherheit auch die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in analoger Form schützt, ist dies im Kontext der Cybersicherheit nicht korrekt. Die Vermischung von Cybersicherheit mit allgemeinem Informationsschutz schafft unnötige Komplexität und administrative Lasten.

Der letzte Satz in Anlage 2 Abschnitt 1, Ziffer 1.1.2 („Zusätzlich gehören dazu analoge Daten [...]") ist zu streichen.

2. KIKS praxisnah definieren – Bekannte Versender

Die für die Luftsicherheit relevanten KIKS unterscheiden sich erheblich zwischen den Akteuren der sicheren Lieferkette. Je weiter ein Akteur von Flughafen und Flugbetrieb entfernt ist, desto weniger KIKS liegen tendenziell vor.

Bei bekannten Versendern kann eine Gefährdung der Luftsicherheit grundsätzlich nur durch die physische Manipulation der Ware erfolgen. Damit eine Manipulation möglich ist, müssen zwei Bedingungen erfüllt sein: Zum einen muss die betreffende Person wissen, dass es sich bei der jeweiligen Sendung um Luftfracht handelt, und zum anderen ist ein physischer Zugang zu identifizierbarer Luftfracht erforderlich. Nur wenn beide Voraussetzungen gegeben sind, besteht ein realistisches Risiko für die Sicherheit der Lieferkette.

Alle Personen bei einem bekannten Versender, die Zugang zu identifizierbarer Luftfracht haben oder diesen erlangen können, sind sowohl nach Ziffer 11.2.3.9 des Anhangs der DVO (EU) 2015/1998 entsprechend geschult als auch einer Zuverlässigkeitsüberprüfung nach § 7 Luftsicherheitsgesetz unterzogen. Damit ist sichergestellt, dass jede Person am Standort über die erforderliche Qualifikation und behördlich bestätigte Zuverlässigkeit für den Umgang mit sicherheitsrelevanter Luftfracht verfügt. Dies gilt auch für Personen, die den Zugang zu identifizierbarer Luftfracht verwalten.

Im Ergebnis liegt deshalb bei bekannten Versendern kein für die Luftsicherheit relevantes KIKS vor, sondern eher eine mögliche Gefährdung durch Innentäter, die aber bereits ausreichend gesetzlich adressiert wurde. Eine Erweiterung der Betrachtung um Cybersicherheitsrisiken würde zu weiteren Belastungen und damit zu einer Schwächung deutscher Unternehmen im internationalen Wettbewerb führen – ohne jeglichen Gewinn in Bezug auf die Luftsicherheit.

In Anlage 2 Abschnitt 2 sollte klargestellt werden: „Bei bekannten Versendern liegen für die Luftsicherheit relevante KIKS nicht vor, insofern der Zugang zu identifizierbarer Luftfracht durch Schulung (nach Ziffer 11.2.3.9 des Anhangs der DVO (EU) 2015/1998) und Zuverlässigkeitsüberprüfung (nach § 7 Luftsicherheitsgesetz) gesichert ist."

3. Zutrittskontrollsysteme sind Sicherheitskontrollen, keine KIKS

Zutrittskontrollsysteme und die Vergabe von Zutrittsberechtigungen zu Luftsicherheitsbereichen werden im Entwurf als kritische informations- und kommunikationstechnische Systeme (KIKS) im geforderten „Cybersicherheitsprogramm" eingestuft.

Die Vergabe von Zutrittsberechtigungen zu Luftsicherheitsbereichen wird vom LBA jedoch als sogenannte „Sicherheitskontrolle" eingestuft, nicht als KIKS. Die Vermischung dieser beiden Kategorien schafft Rechtsunsicherheit.

Zutrittskontrollsysteme zu Luftsicherheitsbereichen sind nicht als KIKS einzuordnen, sondern als Sicherheitskontrollen. Eine praxisnahe Definition von KIKS ist notwendig, die zwischen Akteuren der Lieferkette differenziert.

4. Doppelstrukturen bei Cybersicherheit vermeiden

Die Anforderungen an die Cybersicherheit im Luftverkehr und in der sicheren Lieferkette sollten in einem ganzheitlichen Konzept definiert werden. Dabei müssen sämtliche Vorgaben aus der Durchführungsverordnung (EU) 2019/1583 und dem künftigen NIS2-Umsetzungsgesetz (NIS2UmsuCG) berücksichtigt und in ein integriertes Sicherheitsmanagementsystem überführt werden. Dieses Konzept soll sowohl technische als auch organisatorische Maßnahmen enthalten, beispielsweise ein systematisches Risikomanagement, die Identifizierung und den Schutz kritischer Informations- und Kommunikationstechnik sowie klare Schulungs- und Kontrollprozesse für alle beteiligten Unternehmen der Lieferkette.

Konkret: Die Anforderungen in Anlage 2 Abschnitt 1 NLspV gehen deutlich über die bisherige Praxis hinaus. Sie verlangen Maßnahmen nach BSI-Grundschutz und eine 24-Stunden-Meldepflicht bei erheblichen Störungen (§ 1 Abs. 2 Nr. 2 i. V. m. BSIG § 5b). Dies überschneidet sich mit bestehenden Pflichten aus dem IT-Sicherheitsgesetz (BSIG) und der NIS2-Richtlinie.

Eine Harmonisierung der Meldepflichten mit der NIS2-Richtlinie und dem BSIG erscheint sinnvoll. Unternehmen, die unter die NIS2 fallen, sollten Befugnis erhalten, über ein einheitliches Meldeportal, wie das BSI-Portal, ihre Meldungen zentral einzureichen. Für die Anpassung dieser Prozesse sind Übergangsfristen von mindestens 18 Monaten zu empfehlen. Die Meldepflicht sollte sich klar auf erhebliche Sicherheitsvorfälle beschränken, wie in der NIS2 definiert, und Bagatellfälle, etwa abgefangene Phishing-Mails, sollten ausdrücklich ausgenommen werden, um den bürokratischen Aufwand für Unternehmen zu minimieren.

Die Aufsichtsbehörden sollten dabei die Möglichkeit erhalten, die Gleichwertigkeit mit NIS2-Anforderungen gemäß Nummer 1.7.5 des Anhangs der Durchführungsverordnung (EU) 2015/1998 zu prüfen, um redundante Strukturen und Mehrfachanforderungen zu vermeiden.

5. Anerkennung von KMU-Cybersicherheitslösungen

Bei Bezug auf den BSI-Standard, DIN-ISO 27xxx etc. ist zu berücksichtigen, dass gerade Klein- und mittelständische Unternehmen wirksame und passende Lösungen zu Cybersicherheit umsetzen, jedoch nicht extern zertifiziert sind.

Unternehmen sollten nachweisen können, dass sie wirksame Cybersicherheitsmaßnahmen umsetzen, auch ohne formale externe Zertifizierung. Das LBA sollte bei Inspektionen bewerten, ob die Maßnahmen dem Schutzzweck entsprechen. Eine externe Zertifizierung darf kein zwingendes Kriterium sein. Dabei ist die Wirtschaftlichkeit und Leistungsfähigkeit der Unternehmen angemessen zu berücksichtigen. Analog zu § 13 Abs. 2 des KRITIS-Dachgesetzes sollte eine verhältnismäßige Zweck-Mittel-Relation gewährleistet sein.

Zu § 23 Abs. 1 – Sensibilisierung und Förderung der Sicherheitskultur

Entwurfstext:
„Die Sensibilisierung und Förderung der Sicherheitskultur nach Nummer 11.1.11 des Anhangs der Durchführungsverordnung (EU) 2015/1998 ist bei Einstellung sowie fortlaufend durchzuführen. Die fortlaufende Sensibilisierung und Förderung der Sicherheitskultur nach Satz 1 ist mindestens jährlich durchzuführen."

Position des DSLV

Es bleibt unklar, was genau der Begriff „bei Einstellung“ im Zusammenhang mit der Schulung zur Sicherheitskultur bedeutet und wie dieser zeitlich praktisch umzusetzen ist. Eine pragmatische Lösung wäre, dass bereits bei der vorgeschriebenen Luftfrachtsicherheitsschulung nach Nr. 11.2.3.9 der DVO (EU) 2015/1998 auch die Inhalte zur Sicherheitskultur vermittelt werden. In den Folgejahren könnten die Unternehmen dann jährliche interne Unterweisungen durchführen, um das Thema kontinuierlich im Bewusstsein der Beschäftigten zu halten.

§ 23 Abs. 1 sollte präzisiert werden: „Die Sensibilisierung und Förderung der Sicherheitskultur ist vor erstmaliger Aufnahme der Tätigkeit nach erfolgter Einstellung sowie fortlaufend (mindestens jährlich) durchzuführen. Schulungsinhalte können mit bereits erforderlichen Luftfrachtsicherheitsschulungen (nach Nr. 11.2.3.9 des Anhangs der DVO (EU) 2015/1998) kombiniert werden."

Zu § 26 Abs. 3 – Liste über Beförderungsvereinbarungen bei reglementierten Beauftragten
Zu § 29 Abs. 2 – Liste über Beförderungsvereinbarungen bei bekannten Versendern
Zu § 32 Abs. 5 – Listen und Nachweise bei Transporteuren

Entwurfstext (§ 26 Abs. 3):
„Die reglementierten Beauftragten sind verpflichtet, eine Liste über bestehende Beförderungsvereinbarungen mit zugelassenen Transporteuren nach Nummer 6.3.1.9 Absatz 1 Satz 2 des Anhangs der Durchführungsverordnung (EU) 2015/1998 zu führen und diese dem Luftfahrt-Bundesamt auf Verlangen vorzulegen."

Position des DSLV

Die Führung von Listen zugelassener Unternehmen durch regB und bV ist sinnvoll, weil sie den Nachweis eines strukturierten und transparenten Lieferantenmanagements erleichtert. In der Praxis konnte sowohl bei regBs als auch bei bVs im Rahmen der Prüfung des LFSP durch das LBA regelmäßig die Akzeptanz erreicht werden, dass zugelassene Unternehmen über ein organisiertes, meist softwaregestütztes Lieferantenmanagement verfügen. Dadurch behalten sie den Überblick über einsetzbare Dienstleister und bestehende Geschäftsbeziehungen, was zur Sicherheit und Effizienz der Abläufe beiträgt.

Beförderungsvereinbarungen sind rechtliche Vereinbarungen über die Durchführungen von Transporten/Dienstleistungen. Für die Luft(fracht-)Sicherheit ist hier relevant, dass für die Aufrechterhaltung der „Sicherheit in der Lieferkette" nur behördlich zugelassene Unternehmen eingesetzt werden.

Die Regelung sollte klarstellen, dass die Anforderung als erfüllt gilt, wenn registrierte Beauftragte, bekannte Versender und Transporteure über ein softwarebasiertes Lieferanten-Management-System nachweisen, dass ausschließlich behördlich zugelassene Unternehmen eingesetzt werden. Das System muss dem Luftfahrt-Bundesamt ermöglichen, im Rahmen von Inspektionen die Nachvollziehbarkeit sicherzustellen. Zusätzlich sollten die Unternehmen auf Anforderung des LBA-Einsatzlisten vorlegen können.

Diese Lösung spart administrativen Aufwand, ohne die Luftsicherheit zu gefährden. Doppelaufwände und -strukturen sind identisch wie bei Cybersicherheit zu vermeiden.

Ergänzung zu § 32 Abs. 5 (Transporteure):

Da ab 2027 alle zugelassenen Transporteure auch in der „Unionsdatenbank zur Sicherheit in der Lieferkette" (KSDA2) aufgeführt sind, würde durch zusätzliche Listenpflichten nur ein zusätzlicher Aufwand entstehen.

Alle Unternehmen wissen, für welche Kunden sie tätig sind (u. a. anhand ihrer Daten/Softwaresysteme). Das LBA kann die Abfragen der behördlich zugelassenen Unternehmen der „sicheren Lieferkette" in der EU-Datenbank KSDA2 jederzeit nachvollziehen oder wurde informiert, wenn automatisierte Abfragen mit der jeweils eingesetzten Software erfolgen (siehe Genehmigung im Sicherheitsprogramm, z. B. LFSP für regB).

Zu § 28 Abs. 1 – Änderungen des Sicherheitsprogramms von reglementierten Beauftragten
Zu § 31 Abs. 1 – Änderungen des Sicherheitsprogramms von bekannten Versendern
Zu § 34 Abs. 1 – Änderungen des Sicherheitsprogramms von Transporteuren

Entwurfstext (§ 28 Abs. 1):
„Der Antrag auf Änderung der Zulassung ist im Fall kleinerer Änderungen mindestens 7 Arbeitstage und im Fall größerer Änderungen mindestens 15 Arbeitstage vor dem geplanten Zeitpunkt des Wirksamwerdens der Änderungen unter Vorlage des geänderten Sicherheitsprogramms zu stellen. Das Luftfahrt-Bundesamt kann im Ausnahmefall von der Frist in Satz 4 abweichende Vorgaben anordnen."

Position des DSLV

1. Bürokratieabbau durch Anzeigeverfahren

Änderungen des Sicherheitsprogramms sind nach § 13 Abs. 2, § 19 Abs. 2, § 28 Abs. 1 und § 31 Abs. 1 NLspV genehmigungspflichtig. Das verlangsamt betriebliche Anpassungen an neue Bedrohungslagen erheblich.

Für nicht wesentliche Änderungen sollte ein Anzeigeverfahren mit stillschweigender Zustimmung nach 10 Arbeitstagen gelten.

2. Verlässliches Rückmelde-System des LBA erforderlich

Das Problem besteht darin, dass Unternehmen vom Luftfahrt-Bundesamt (LBA) häufig über Wochen oder sogar gar nicht darüber informiert werden, ob eine beantragte Änderung genehmigt bzw. der jeweilige Prozess freigegeben wurde. Diese ausbleibende oder verspätete Rückmeldung führt zu erheblicher Unsicherheit bei den Unternehmen, da nicht klar ist, ab wann mit teilweise zeitkritischen Umstellungen rechtssicher begonnen werden darf.

Das Luftfahrt-Bundesamt (LBA) sollte ein verlässliches Rückmeldesystem einführen, das verbindliche Bestätigungen innerhalb von zehn Arbeitstagen gewährleistet. Unternehmen müssen dabei klare Gewissheit darüber haben, zu welchem Zeitpunkt eine Genehmigung als wirksam gilt, um Planungssicherheit und rechtsverbindliche Abläufe sicherzustellen.

3. Konsistenz der Genehmigungsfristen

§ 28 Abs. 1 (regB) fordert 7/15 Arbeitstage, während § 34 Abs. 1 (Transporteure) 10/15 Arbeitstage vorsieht. Dies ist inkonsistent.

Die Genehmigungsfristen sollten zwischen § 28 (regB), § 31 (bV) und § 34 (Transporteure) harmonisiert werden. Einheitlich sollten 10 Arbeitstage (kleinere Änderungen) und 15 Arbeitstage (größere Änderungen) gelten.

Zu § 33 Abs. 2 – Sprachanforderungen für Sicherheitsprogramme der Transporteure

Entwurfstext:
„Transporteure sind verpflichtet, ihr Sicherheitsprogramm in deutscher Sprache vorzulegen. Die englischsprachige Fassung im Sinne von Nummer 6.5.1.2 Absatz 3 Satz 2 des Anhangs der Durchführungsverordnung (EU) 2015/1998 darf inhaltlich nicht von der deutschsprachigen Fassung abweichen."

Position des DSLV

Diese Verpflichtung ist in den heutigen Zeiten und mit frei zugänglichen, sehr guten Übersetzungs-Tools fragwürdig. Das Luftfrachtgeschäft ist international, und Englisch ist eine gängige Arbeitssprache.

Das Cybersecurity Programm wird in einigen zugelassenen Unternehmen aufgrund der IT/IS-Sprache auf Englisch erstellt (da auch konzernweit gültig). Es ist in einem bekannten Fall eine Nachforderung seitens LBA eingegangen, das Cybersecurity Programm auf DEUTSCH einzureichen. IT-Prozesse zu übersetzen, macht hier oft wenig Sinn.

Unternehmen sollten die Möglichkeit haben, Sicherheitsprogramme oder Teile davon, insbesondere IT- und Cybersecurity-Anlagen, in englischer Sprache einzureichen. Das Luftfahrt-Bundesamt (LBA) kann Übersetzungen anfordern, wenn diese für die Prüfung oder Kontrolle erforderlich sind. Diese Regelung sollte insbesondere für § 33, der Transporteure betrifft, sowie für Cybersecurity-Programme nach Anlage 2 gelten.

Zu §§ 33–36 – Zulassungsverfahren für Transporteure ab 1. Januar 2027
Zu § 46 – Übergangsvorschriften

Entwurfstext (§ 46 Abs. 1):
„Abschnitt 4 Unterabschnitt 4 findet erst Anwendung auf Zulassungen von Transporteuren nach § 9a Absatz 2 des Luftsicherheitsgesetzes in Verbindung mit Nummer 6.5 des Anhangs der Durchführungsverordnung (EU) 2015/1998, die mit Wirkung zum 1. Januar 2027 oder einem späteren Zeitpunkt erteilt werden."

Position des DSLV

1. Vermeidung von Doppelgenehmigungen

Kernfrage: Muss jeder bereits behördlich zugelassene Transporter einen vollständig neuen Approval-Prozess durchlaufen und sich als „Haulier" gemäß EU-Anforderungen neu zertifizieren lassen?

Es sollte vermieden werden, dass alle bereits behördlich zugelassenen „Transporteure" nochmals einen neuen Approval-Prozess/Zertifizierung als „Haulier" durchlaufen. Die bestehenden LBA-Zulassungen auf Basis des „Transporter Security Programme" sollten weiterhin berücksichtigt werden.

Die Aufwände (u. a. finanziell und zeitlich) für die Unternehmen mit LBA-Zulassung sollten nicht weiter erhöht werden. Die 9. LuftSiGebV (Gebühren-VO) und sonstige hohe Standortkosten in Deutschland sind bereits herausfordernd und führen zu Wettbewerbsverlusten im internationalen Wettbewerb.

Argumentation zum Schutzzweck:
Ab 2027 sind alle zugelassenen Transporteure ohnehin in der „Unionsdatenbank zur Sicherheit in der Lieferkette" (KSDA2) registriert. Das LBA kann automatisierte Abfragen der behördlich zugelassenen Transporte durchführen oder wird informiert, wenn Unternehmen ihre genehmigten Systeme einsetzen (z. B. im LFSP). Ein zusätzlicher Approval-Prozess für bereits zugelassene Transporteure schafft nur Redundanz und Mehraufwand.

§ 46 sollte klarstellen, dass bestehende Zulassungen des Luftfahrt-Bundesamts auf Basis des „Transporter Security Programme“ beim Übergang in das neue System berücksichtigt werden. Für bereits zugelassene Transporteure sollte ein vereinfachter Registrierungsprozess anstelle eines vollständigen neuen Approvals gelten. Zudem sollten die Kostenbelastungen möglichst geringgehalten werden, um Wettbewerbsnachteile für betroffene Unternehmen zu vermeiden.

2. Übergangsfristen

Eine angemessene Übergangsfrist von mindestens 18 bis 24 Monaten vor dem 1. Januar 2027 sollte in § 46 verankert werden. Zudem sollte das Luftfahrt-Bundesamt (LBA) rechtzeitig Mustervorlagen und Guidelines spätestens sechs Monate vor Beginn der Übergangsfrist bereitstellen. Unternehmen, die bereits über ein bestehendes Approval verfügen, sollten durch vereinfachte Verfahren entlastet werden, um den Umstellungsaufwand zu minimieren.

Zu § 40 – Validierungs- und Dokumentationspflichten für bekannte Lieferanten und Transporteure

Entwurfstext (§ 40 ff.):
Umfangreiche Validierungs- und Dokumentationspflichten für bekannte Lieferanten von Bordvorräten und Flughafenlieferungen.

Position des DSLV

Die Validierungs- und Dokumentationspflichten für bekannte Lieferanten und Transporteure sind sehr umfangreich. Um unnötige Bürokratie zu vermeiden, sollten bestehende internationale Standards wie ISO 9001 oder ISAGO als gleichwertig anerkannt werden. Darüber hinaus sollten Re-Validierungen überwiegend dokumentenbasiert durchgeführt werden, um Doppelprüfungen zu vermeiden und den Aufwand für Unternehmen zu reduzieren.

Zu Anlage 2 – Informationssicherheitsmaßnahmen: Weitere Regelungen
Zu Anlage 2 Abschnitt 1, Ziffer 3.1 – Zuverlässigkeitsüberprüfung (ZÜP) für Personen mit Administrator-Rechten

Entwurfstext:
„Personen mit Administrator-Rechten [...] mussen eine erweiterte Zuverlässigkeitsüberprüfung [...] erfolgreich abgeschlossen haben."

Position des DSLV

Der Entwurf verlangt, dass Personen mit Administrationsrechten (unabhängig vom Wohnsitz) einer deutschen erweiterten ZÜP unterzogen werden. Dies ist für Personen außerhalb der EU unzweckmäßig und praktisch nicht erfüllbar.

Unternehmen lagern IT-Dienstleistungen häufig an Softwareunternehmen außerhalb der EU aus. Eine erweiterte Zuverlässigkeitsüberprüfung (ZÜP) durch deutsche Behörden ist für solche Personen jedoch oft nicht möglich. Daher sollte das Luftfahrt-Bundesamt (LBA) Regelungen schaffen, wie die Zuverlässigkeit von im Ausland ansässigen Personen bestätigt werden kann. Eine gegenseitige Anerkennung von Zuverlässigkeitsüberprüfungen zwischen EU-Mitgliedstaaten sollte dabei geprüft werden. Ebenso sollten Staaten mit als gleichwertig anerkannten Sicherheitsstandards, wie etwa die USA oder das Vereinigte Königreich, akzeptiert werden. Für Personen aus anderen Ländern sollten alternativ geeignete Sicherheitsmaßnahmen wie spezielle Datenschutzverträge, Einschränkungen beim Fernzugriff oder begleitete Fernwartung herangezogen werden.

Zu Anlage 2 Abschnitt 1, Ziffer 3.1 – Protokollierung von Administratorenzugriffen

Entwurfstext:
„Alle Zugriffe und Tätigkeiten sind zu protokollieren [...]. Im Anschluss hat eine Überprüfung der Protokolldaten zu erfolgen, die zu dokumentieren ist."

Position des DSLV

Diese Anforderung ist zu umfassend, ohne dass ein echter Sicherheitsgewinn erzielt wird. Das Protokollieren aller Systemzugriffe erzeugt enorme Datenmengen, wobei nicht jeder Zugriff relevant für die Luftsicherheit ist. Eine automatisierte Protokollierung sämtlicher Aktionen ist zudem technisch aufwendig und ressourcenintensiv. Es sollte daher ein risikobasierter und datensparender Ansatz verfolgt werden. Die Protokollierungspflicht sollte sich auf begründete Risikobereiche oder relevante Personenkreise beziehen, etwa beim Zugriff auf Luftsicherheitsdatenbanken und nicht bei allen Systemaktivitäten. Unternehmen sollten ihre Risk-based-Ansätze dokumentieren und dem LBA offenlegen.

Zu Begründung „E.2 Erfüllungsaufwand für die Wirtschaft"

Entwurfstext:
„Das geplante Regelungsvorhaben der Bundesregierung führt für den Normadressaten Wirtschaft zu keiner Änderung des Erfüllungsaufwands."

Position des DSLV

Diese Abschätzung ist nicht nachvollziehbar. Die NLspV droht in ihrer gegenwärtigen Form in erheblichem Mehraufwand bei betroffenen Unternehmen zu resultieren: Es kommen neue Cybersicherheitsanforderungen in Anlage 2 hinzu, genehmigungspflichtige Programmänderungen, neue Validierungs- und Dokumentationspflichten, gegebenenfalls neue Zulassungsverfahren für Transporteure ab 2027 und gebührenpflichtige Änderungen von Sicherheitsprogrammen. Der Erfüllungsaufwand sollte realistisch dargestellt und korrigiert werden, da die Abschätzung „keine Änderung des Erfüllungsaufwands“ unzutreffend ist und im weiteren Verfahren angepasst werden muss.

Schlussbemerkung

Der DSLV setzt sich für eine praxisgerechte Nationale Luftsicherheitsprogramm-Verordnung ein, die die europäischen Vorgaben rechtssicher umsetzt, ohne deutsche Unternehmen mit redundanten Anforderungen zu belasten. Die Unternehmen der sicheren Lieferkette verfügen bereits über etablierte Sicherheitskultur, Compliance-Strukturen und IT-Management. Diese sollten anerkannt und genutzt werden – nicht durch zusätzliche Genehmigungsverfahren und Doppelstrukturen unterlaufen werden.

Die hier vorgebrachten Forderungen zielen nicht auf eine Abschwächung der Luftsicherheit ab, sondern auf effiziente, verhältnismäßige und nachvollziehbare Regelungen, die Sicherheit und Wirtschaftlichkeit vereinbaren.

Verbandsstruktur, Leistungsprofil und Leitlinien

Als Spitzen- und Bundesverband vertritt der DSLV über 16 regionale Landesverbände die verkehrsträgerübergreifenden Interessen der deutschen Speditions- und Logistikunternehmen. Diese sind mit insgesamt 600.000 Beschäftigten und einem jährlichen Branchenumsatz von 123 Milliarden Euro ein wesentlicher Teil des drittgrößten Wirtschaftsbereichs Deutschlands (Stand: Oktober 2025).

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

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

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

Gemeinsam mit seinen Landesverbänden ist der DSLV Berater und Dienstleister für die Speditions- und Logistikunternehmen. Die Landesverbände vertreten die Branche als Arbeitgeberverbände und Sozialpartner in regionalen Tarifangelegenheiten.

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

Die Mitgliedsunternehmen des DSLV bekennen sich zu den Zielen der Sozialen Marktwirtschaft und der Europäischen Union.