BPEX
BUNDESVERBAND PAKET- UND EXPRESSLOGISTIK

Stellungnahme

Zum Entwurf des Bundesministeriums des Innern (BMI) vom 24.06.2025 zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG)

Berlin, 04. Jul. 2025

Kernpositionen im Überblick

Zu § 30: Um Planungs- und Rechtssicherheit für die betroffenen Einrichtungen zu gewährleisten, sollte klargestellt werden, inwieweit gängige IT-Zertifizierungen wie die ISO-27001 als Nachweis für die Erfüllung der Anforderungen an das Risikomanagement nach § 30 anerkannt werden können. Dies könnte analog zur Begründung des Entwurfs zu § 44 Abs. 2 erfolgen. Zudem sollte das Bundesamt ausdrücklich befähigt werden, derartige Zertifizierungen bei der Bewertung der Erfüllung der Sicherheitsanforderungen dieses Gesetzes zu berücksichtigen. Darüber hinaus sollte wichtigen Einrichtungen die Möglichkeit eingeräumt werden, dem Bundesamt branchenspezifische Sicherheitsstandards vorzuschlagen.

Zu § 32, § 33 und § 40: Um dem Ziel der Bürokratieentlastung gerecht zu werden, muss klar sichergestellt sein, dass bei grenzüberschreitenden Sicherheitsvorfällen die Meldepflicht nach § 32 ausschließlich gegenüber einer nationalen Meldestelle innerhalb der EU besteht. Andernfalls droht Unternehmen eine unverhältnismäßige Mehrbelastung durch parallele Meldepflichten. Außerdem sollte nur dann das vorgesehene dreistufige Meldesystem nach § 32 ausgelöst werden, wenn der betroffenen Einrichtung nach einer sachgerechten Bewertung durch eine fachlich qualifizierte Person eine „substantiierte" Kenntnis über einen erheblichen Sicherheitsvorfall vorliegt.

Zu § 35: Vor einer Anordnung zur Unterrichtung der Empfänger durch das Bundesamt sollte eine verbindliche Abstimmung mit der betroffenen Einrichtung erfolgen. Ziel dieser Abstimmung muss es sein, die Verhältnismäßigkeit der Maßnahme zu prüfen und sicherzustellen, dass eine Unterrichtung nur in solchen Fällen erfolgt, in denen sie für die Empfänger tatsächlich relevant ist – um vermeidbare Reputationsschäden zu verhindern.

Zu § 38: Die derzeitige Auslegung berücksichtigt nicht die organisatorischen Gegebenheiten international tätiger Konzerne, in denen IT-Systeme zentral gesteuert und überwacht werden. § 38 sollte daher dahingehend präzisiert werden, dass die nationale Geschäftsleitung lediglich zur Kenntnisnahme und regelmäßigen Unterrichtung über relevante Risikomanagementmaßnahmen verpflichtet ist. Es wäre sachgerechter, wenn die Verantwortung für die Pflichten nach § 38 ausschließlich bei den konzernintern zuständigen Geschäftsleitern und Entscheidungsträgern im Bereich des IT-Risikomanagements läge.

Zu § 56: Die Einbindung der Wirtschaftsverbände bzw. ihrer Mitglieder ist bei der Ausarbeitung von Rechtsverordnungen nach § 56 Abs. 4 zwingend erforderlich. Ihre fachliche Expertise ist entscheidend, um praxistaugliche und wirtschaftlich tragfähige Bemessungsgrößen zur Festlegung von Schwellenwerten und zur Bestimmung des Versorgungsgrads zu entwickeln sowie wirtschaftliche Nachteile für die betroffenen Unternehmen zu minimieren. Eine gesetzliche Verpflichtung zur Anhörung der Verbände sollte daher ausdrücklich vorgesehen werden. Um die Kohärenz des Rechtsrahmens zu

sichern und Rechtsunsicherheiten zu vermeiden, ist es zudem notwendig, dass die Bemessungsgrößen in allen einschlägigen Rechtsvorschriften einheitlich geregelt werden.

Zu § 60: Es ist unklar, ob die in § 60 Abs. 3 genannten Verpflichtungen auch für andere besonders wichtige Einrichtungen gelten, die nicht in § 60 Abs. 1 aufgeführt sind. Wir empfehlen, diese Frage eindeutig zu regeln, um eine bessere Planung und Umsetzung zu ermöglichen.

Zu § 62: Maßnahmen und Offenlegungspflichten nach § 61 sollten nur dann angeordnet werden können, wenn zuvor eine fundierte Einschätzung der möglichen Defizite bei der Umsetzung der Pflichten der jeweiligen Einrichtung vorgenommen wurde. Der betroffenen Einrichtung muss die Gelegenheit zur Stellungnahme gegeben werden, damit sie etwaige Zweifel frühzeitig ausräumen kann.

Zu Artikel 29: Um den Unternehmen ausreichend Zeit für eine gründliche Planung und Umsetzung zu ermöglichen, sollte der Gesetzentwurf einheitliche Umsetzungsfristen von mindestens drei Jahren ab Inkrafttreten vorsehen – entsprechend der bereits in § 61 Abs. 3 festgelegten Frist für besonders wichtige Einrichtungen.

Zu Anlage 1 Spalte A Nr. 2.1.2: Derzeit ist unklar, nach welchen Kriterien „Einrichtungen, die innerhalb von Flughäfen befindliche Einrichtungen betreiben", dem Sektor „besonders wichtiger Einrichtungen zugeordnet werden. Wir empfehlen klarzustellen, dass nur solche Einrichtungen innerhalb von Flughäfen unter das Gesetz fallen, die zum eigentlichen Flugbetrieb gemäß der EU-Richtlinie 2009/12/EG gehören. Andernfalls würden auch Unternehmen erfasst, die lediglich Fracht an Flughäfen verladen, ohne die relevante IT-Infrastruktur des Flughafens zu nutzen.

Zu Anlage 2: Um zu vermeiden, dass die Anforderungen des NIS2UmsuCG implizit zu einer Marktzugangsvoraussetzung oder gar zu einer Eintrittsbarriere für den Markt der Postdienstleistungen werden, sollte dringend der Kreis der betroffenen Unternehmen als „wichtige Einrichtungen" gemäß der Anlage 2 für die Branche „Post- und Kurierdienste" präzisiert werden. Post- und Kurierdienstleister sollten nur dann unter die Regelungen des NIS2UmsuCG fallen, wenn sie Post- oder Kurierdienste in eigenem Namen erbringen.

Erläuterungen der Kernpositionen

Zu § 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Sowohl besonders wichtige als auch wichtige Einrichtungen sind verpflichtet, Risikomanagementmaßnahmen zum Schutz vor potenziellen Sicherheitsrisiken in der Informationstechnik zu ergreifen (§ 30 Abs. 1). Um Planungs- und Rechtssicherheit für die betroffenen Einrichtungen zu gewährleisten, sollte klargestellt werden, inwieweit gängige IT-Sicherheitszertifikate, wie beispielsweise die ISO-27001-Zertifizierung, als Nachweis für die Erfüllung der Risikomanagementanforderungen nach § 30 anerkannt werden können. Eine solche Regelung könnte analog zur Begründung des Entwurfs zu § 44 Abs. 2 erfolgen, in der festgelegt wird, dass Einrichtungen der Bundesverwaltung die Erfüllung der Mindestanforderungen unter anderem durch ein ISO-27001-Zertifikat belegen können. Das Bundesamt sollte aus diesem Grund dazu befähigt werden, allgemeine IT-Zertifizierungen, wie die ISO-27001, für alle Einrichtungskategorien als Nachweis der Erfüllung der Sicherheitsanforderungen nach § 30 berücksichtigen zu können.

Darüber hinaus haben besonders wichtige Einrichtungen, deren Branchenverbände und Betreiber kritischer Anlagen die Möglichkeit, branchenspezifische Sicherheitsstandards zur Erfüllung der Anforderungen nach § 30 Abs. 1 vorzuschlagen. Das Bundesamt prüft auf Antrag, ob die vorgeschlagenen Standards branchenspezifisch und geeignet sind. Diese Möglichkeit sollte auch für wichtige Einrichtungen und ihre Branchenverbände gelten. Es bestehen keine Einwände gegen Vorschläge für branchenspezifische Sicherheitsstandards für wichtige Einrichtungen, sofern diese die Durchführungsrechtsakte der Europäischen Kommission berücksichtigen, mit den darin enthaltenen Anforderungen übereinstimmen und nicht hinter diesen zurückbleiben. Schließlich sind die jeweiligen Einrichtungen am besten in der Lage, unter Berücksichtigung der Besonderheiten ihrer Branche, geeignete Maßnahmen zum Schutz ihrer IT-Sicherheit zu ermitteln, ohne ihre Wettbewerbsfähigkeit zu beeinträchtigen.

Zu § 32 Meldepflichten, § 33 Registrierungspflicht und § 40 Nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für besonders wichtige und wichtige Einrichtungen

Positiv hervorzuheben ist, dass gemäß der Begründung zu § 33 Absatz 1 innerhalb einer Konzerngruppe bei der Registrierung der Einrichtungen nur eine zentrale Kontaktstelle für meldepflichtige Sicherheitsvorfälle benannt werden muss. Diese Kontaktstelle ist gemäß § 32 und dessen Begründung befugt, Sicherheitsvorfälle für alle Einrichtungen des Konzerns an die jeweils zuständige Meldestelle – auch in englischer Sprache – zu melden. Dies trägt erheblich zur Reduzierung des administrativen Aufwands bei.

Um dem Ziel der Bürokratieentlastung weiterhin gerecht zu werden, muss klar sichergestellt sein, dass bei grenzüberschreitenden Sicherheitsvorfällen die Meldepflicht nach § 32 ausschließlich gegenüber einer nationalen Meldestelle innerhalb der EU besteht, um Doppelmeldungen zu vermeiden. Eine entsprechende Präzisierung ist erforderlich, um den Meldeprozess rechtssicher, effizient und eindeutig zu gestalten. Andernfalls droht Unternehmen eine unverhältnismäßige Mehrbelastung durch parallele Meldepflichten. Den aktuellen Entwurf von § 40, insbesondere Absatz 3 Nr. 4, verstehen wir so, dass die Weiterleitung grenzüberschreitender Meldungen an andere betroffene Mitgliedstaaten

durch das Bundesamt in seiner Funktion als zentrale Meldestelle erfolgt. In diesem Fall sollte klargestellt werden, dass eine einmalige Meldung beim Bundesamt ausreicht.

Das vorgesehene dreistufige Meldesystem wird gemäß § 32 „nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall" ausgelöst. Laut der entsprechenden Begründung ist mit „Kenntniserlangung" gemeint, „dass eine Mitarbeiterin oder ein Mitarbeiter der Einrichtung innerhalb seiner Arbeitszeit Kenntnis über einen erheblichen Sicherheitsvorfall erlangt". Um jedoch beurteilen zu können, ob es sich tatsächlich um einen erheblichen Sicherheitsvorfall im Sinne des Gesetzes handelt, sind hinreichende Fachkenntnisse sowie eine erste Analyse des Vorfalls und seiner Ursachen erforderlich. Daher ist klarzustellen, dass nicht jede bloße Information oder Vermutung eine Meldepflicht auslöst, sondern erst dann, wenn auf Grundlage einer sachgerechten Bewertung eine „substantiierte" Kenntnis vorliegt. Dies stellt sicher, dass die Meldepflichten nach § 32 erst dann greifen, wenn die Einrichtung nachweislich durch die Bewertung von sachlich qualifizierten Personen davon ausgehen kann, dass ein erheblicher Sicherheitsvorfall tatsächlich vorliegt – und nicht bereits bei bloßem Anfangsverdacht.

Zu § 35 Unterrichtungspflichten

Die gesetzlich vorgesehene Pflicht zur Unterrichtung der Empfänger von Diensten besonders wichtiger und wichtiger Einrichtungen über erhebliche Sicherheitsvorfälle kann erhebliche Reputationsschäden zur Folge haben – selbst dann, wenn die tatsächliche Gefährdung für die betroffenen Empfänger als gering einzustufen ist. Daher ist es dringend erforderlich, dass vor einer entsprechenden Anordnung durch das Bundesamt eine verbindliche Abstimmung mit der betroffenen Einrichtung stattfindet. Ziel dieser Abstimmung muss es sein, die Verhältnismäßigkeit der Maßnahme zu prüfen und sicherzustellen, dass eine Unterrichtung der Empfänger ausschließlich in Fällen erfolgt, in denen diese für sie tatsächlich relevant ist.

Zu § 38 Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Gemäß § 38 Abs. 1 sind die Geschäftsleitungen besonders wichtiger und wichtiger Einrichtungen verpflichtet, „die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen". Diese Regelung berücksichtigt jedoch nicht die organisatorische Realität international tätiger Konzerne, in denen IT-Systeme häufig zentral gesteuert und überwacht werden. In solchen Fällen liegt das IT-Risikomanagement in der Regel nicht in der Verantwortung der nationalen Geschäftsleitungen, die daher auch nicht befugt sind, entsprechende Maßnahmen eigenständig umzusetzen. Stattdessen nehmen sie die konzernweit umgesetzten Risikomanagementmaßnahmen zur Kenntnis und werden über deren Implementierung im Rahmen zentraler Prozesse informiert. Vor diesem Hintergrund sollte § 38 dahingehend präzisiert werden, dass die nationale Geschäftsleitung nicht zur unmittelbaren Umsetzung, sondern nur zur Kenntnisnahme und regelmäßigen Unterrichtung über relevante Maßnahmen verpflichtet ist.

Insbesondere in zentralen Stabsstellen eines Konzerns ist das Fachwissen über die Struktur und Funktionsweise der konzernweiten IT-Systeme gebündelt. Es wäre daher sachgerechter, wenn die Verantwortung für die Umsetzungs-, Überwachungs- und

Schulungspflichten gemäß § 38 ausschließlich bei den konzernintern zuständigen Geschäftsleitern und Entscheidungsträgern im Bereich IT-Risikomanagement läge.

Zu § 56 Ermächtigung zum Erlass von Rechtsverordnungen

Gemäß § 56 Abs. 4 und der dazugehörigen Begründung soll durch Rechtsverordnung festgelegt werden, welche Anlagen als kritische Anlagen im Sinne dieses Gesetzes gelten. Grundlage hierfür sind die in § 2 Nr. 24 genannten Sektoren sowie die darin erbrachten, als kritisch eingestuften Dienstleistungen und deren jeweiliger als bedeutend angesehener Versorgungsgrad. Dieser Versorgungsgrad soll durch branchenspezifische Schwellenwerte für jede als kritisch eingestufte Dienstleistung bestimmt werden.

Unverständlich ist, weshalb beim Erlass der Rechtsverordnung gemäß § 56 Abs. 4 keine Anhörung der betroffenen Wirtschaftsverbände vorgesehen ist. Die Festlegung, welche Anlagen als kritisch im Sinne dieses Gesetzes gelten, hat direkte Auswirkungen darauf, ob betroffene Unternehmen den erhöhten Sicherheitsanforderungen des vorliegenden Entwurfs unterliegen. Dies kann mit erheblichen administrativen Kosten verbunden sein und sich negativ auf ihre Wettbewerbsfähigkeit auswirken. Angesichts dieser weitreichenden Folgen – nicht nur für einzelne Branchen, sondern für ganze Wirtschaftszweige – ist eine Einbeziehung der entsprechenden Verbände unerlässlich. Neben ihrer Betroffenheit verfügen diese auch über die fachliche Expertise, um geeignete Bemessungsgrundlagen zur Festlegung von Schwellenwerten und des Versorgungsgrades zu ermitteln. Ihre Einschätzung ist entscheidend, um praxistaugliche und verhältnismäßige Regelungen zu gewährleisten. Daher sollte gesetzlich vorgesehen werden, dass betroffene Wirtschaftsverbände bei der Ausarbeitung von Rechtsverordnungen nach § 56 Abs. 4 zwingend angehört werden.

Weiterhin wird angemerkt, dass die Bestimmung von KRITIS-Betreibern im Rahmen dieses Gesetzes im Einklang mit dem KRITIS-Dachgesetz und dem in jahrelanger Verwaltungspraxis etablierten Verfahren der Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) erfolgen soll. Wir möchten hier nachdrücklich betonen, dass die Bemessungsgrößen, auf deren Grundlage Schwellenwerte festgelegt und der Versorgungsgrad durch die von einer Anlage versorgten Personen bestimmt wird, in allen Rechtsrahmen einheitlich geregelt werden müssen. Dies ist entscheidend, um die Kohärenz der Rechtsvorschriften zu gewährleisten und Rechtsunsicherheiten zu vermeiden.

Zu § 60 Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten

Der vorliegende Entwurf verpflichtet in § 60 Abs. 3 lediglich die in § 60 Abs. 1 genannten Einrichtungen, die Dienstleistungen innerhalb der Europäischen Union anbieten, jedoch nicht in einem Mitgliedstaat niedergelassen sind, zur Benennung eines Vertreters. Dieser Vertreter muss in dem Mitgliedstaat ansässig sein, in dem die betreffende Einrichtung ihre Dienste erbringt. Unklar bleibt jedoch, ob diese Verpflichtung auch für andere besonders wichtige Einrichtungen gilt. Zur Sicherstellung einer einheitlichen Anwendung und zur Unterstützung der betroffenen Einrichtungen bei Planung und Umsetzung empfehlen wir, diese Frage eindeutig zu regeln.

Zu § 62 Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen

Gemäß § 62 kann das Bundesamt bereits dann Aufsichts- und Durchsetzungsmaßnahmen nach § 61 anordnen, wenn die Annahme besteht, dass eine wichtige Einrichtung ihren Verpflichtungen nach § 30 Absatz 1 Satz 1, § 32 Absatz 1 bis 3 oder § 38 Absatz 3 nicht oder nicht richtig umsetzt. Pauschale Annahmen reichen hierfür jedoch nicht aus, da sie keine belastbare Grundlage für eine umfassende Bewertung bieten. Die Einführung, Umsetzung und Aufrechterhaltung von IT-Sicherheitsstandards erfordern regelmäßig komplexe und zeitintensive Geschäftsprozesse. In der derzeitigen Regelung sehen sich Unternehmen der Gefahr ausgesetzt, aufgrund vorschneller oder unzutreffender Annahmen mit Maßnahmen und Offenlegungspflichten nach § 61 konfrontiert zu werden. Um derartigen Fehlentwicklungen vorzubeugen, sollte die Anordnung von Maßnahmen nach § 61 nur dann zulässig sein, wenn zuvor eine fundierte Einschätzung über die möglichen Defizite bei der Umsetzung der Pflichten erfolgt ist. Der betroffenen Einrichtung ist in diesem Zusammenhang die Gelegenheit zur Stellungnahme zu geben, sodass sie etwaige Zweifel frühzeitig ausräumen kann.

Zu Artikel 29 Inkrafttreten, Außerkrafttreten

Die Umsetzung des vorliegenden Gesetzesentwurfs ist komplex und bedarf einer sorgfältigen Planung. Dazu gehören die Analyse, Bewertung und Priorisierung des konkreten Handlungsbedarfs sowie die Beschaffung und Integration personeller und materieller Ressourcen. Darüber hinaus müssen Mitarbeitende geschult und neue Prozesse eingeführt werden, begleitet von umfangreichen Kommunikationsmaßnahmen. Für international aufgestellte Konzerne ist der Aufwand weitaus höher, da die NIS-2-Richtlinie sämtliche europäischen Landesgesellschaften erfasst und die Umsetzung je nach nationaler Gesetzgebung unterschiedlich ausfallen kann. Dies macht eine länderübergreifende Koordination der IT-Systeme innerhalb des Konzerns sowie eine jeweils nationale Analyse zur Anpassung an die spezifischen Anforderungen der Mitgliedstaaten erforderlich. Um Unternehmen ausreichend Zeit für eine gründliche Planung und Umsetzung zu geben, sollte der Gesetzentwurf einheitliche Umsetzungsfristen von mindestens drei Jahren ab Inkrafttreten vorsehen – analog zu der bereits in § 61 Absatz 3 vorgesehenen Frist für besonders wichtige Einrichtungen.

Zu Anlage 1 Sektoren besonders wichtiger und wichtiger Einrichtungen

In der Anlage 1 Spalte A Nr. 2.1.2 ist zurzeit unklar, nach welchen Kriterien „Einrichtungen, die innerhalb von Flughäfen befindliche Einrichtungen betreiben", dem Sektor „besonders wichtiger Einrichtungen zugeordnet werden. Wir empfehlen zu konkretisieren, dass Einrichtungen innerhalb von Flughäfen nur dann vom Anwendungsbereich des Gesetzes erfasst werden, wenn sie als Einrichtungen im Sinne der Definition eines „Flughafens" nach Artikel 2 Nr. 1 der Richtlinie 2009/12/EG zu verstehen sind. Anders ausgedrückt, die Definition von "Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben" sollte eng an den Kernbereich des Flugbetriebs geknüpft werden. Ansonsten würden auch Logistikunternehmen, die lediglich ihre Fracht an Flughäfen verladen, ohne auf die IT-Infrastruktur des Flughafens angewiesen zu sein, fälschlicherweise unter die Regelung für „besonders wichtige Einrichtungen" fallen.

Zu Anlage 2 Sektoren wichtiger Einrichtungen

Die Branche „Post- und Kurierdienste", die in Anlage 2 zur Bestimmung der Sektoren wichtiger Einrichtungen erfasst wird, soll Anbieter von Postdienstleistungen gemäß § 3 Nr. 15 PostG, einschließlich der Anbieter von Kurierdiensten, umfassen. Aufgrund der an das Postgesetz angelehnten Definition würden zahlreiche Transportunternehmen, die mit der Zustellung von Paketsendungen beauftragt werden, in den Anwendungsbereich des NIS2UmsuCG fallen. Viele dieser Unternehmen erfüllen auch die Anforderungen in Bezug auf die Zahl der Mitarbeiter, die Jahresbilanzsumme oder den Jahresumsatz, die für die Einstufung als „wichtige Einrichtung" erforderlich sind.

Die IT-Infrastruktur dieser Transportunternehmen ist jedoch nicht entscheidend für die Versorgungssicherheit der Bevölkerung mit Postdienstleistungen. Sie agieren lediglich als Auftragnehmer für spezifische Aufgaben der Postdienstleister. Die von den Transportunternehmen auf der „letzten Meile" verladenen und entgegengenommenen Sendungen werden ausschließlich im IT-System des jeweiligen Postdienstleisters erfasst. Als Auftragnehmer profitieren sie zwar von der IT-Infrastruktur der Postdienstleister, etwa den Versandsystemen, sind jedoch nicht direkt mit diesen verbunden. Die Postdienstleister betreiben ihre IT-Systeme und -Prozesse eigenständig. Ein potenzieller Ausfall der IT-Systeme der Transportunternehmen hätte daher keine kritischen Auswirkungen auf die Sicherstellung der Postversorgung für Wirtschaft und Gesellschaft.

Vor diesem Hintergrund ist es nicht gerechtfertigt, an die IT-Systeme und -Prozesse der Transportunternehmen, die auf der letzten Meile tätig sind, die umfangreichen Anforderungen zu stellen, die in der aktuellen Fassung des NIS2UmsuCG vorgesehen sind. Eine Einbeziehung dieser Unternehmen in den Anwendungsbereich des Gesetzes würde sie wirtschaftlich, personell sowie hinsichtlich ihrer Qualifikationen und ihres Know-hows überfordern, ohne einen nennenswerten Beitrag zur Cybersicherheit und damit zur Versorgungssicherheit der Postdienstleistungen in Deutschland zu leisten. Vielmehr würde die Einführung solcher Anforderungen für viele Auftragnehmer eine erhebliche Eintrittsbarriere auf den Postmarkt schaffen, was langfristig die Versorgungssicherheit gefährden könnte und zu einer nachhaltigen Störung der postalischen Lieferkette führen würde.

Aus diesen Gründen sollten diese Transportunternehmen nicht als „wichtige Einrichtungen" im Sinne des Gesetzes eingestuft werden. Wir empfehlen dringend, den Kreis der betroffenen Unternehmen, die als „wichtige Einrichtungen" gemäß Anlage 2 für die Branche „Post- und Kurierdienste" gelten, weiter zu präzisieren. Anbieter von Post- und Kurierdiensten sollten nur dann unter die Regelungen des NIS2UmsuCG fallen, wenn sie auch Post- oder Kurierdienste in eigenem Namen erbringen. Andere an der Postversorgung beteiligte Unternehmen werden bereits durch die Anforderungen zur „Sicherheit der Lieferkette" nach § 30 Abs. 2 Nr. 4 ausreichend erfasst. Diese Regelung stellt sicher, dass die Auftraggeber die Austauschbeziehungen mit ihren Dienstleistern resilient gestalten, was geeignete Risikomanagementmaßnahmen einschließt.

Der Bundesverband Paket- und Expresslogistik

Der 1982 gegründete Bundesverband Paket- und Expresslogistik (BPEX) vertritt die Interessen der Kurier-, Express- und Paketbranche (KEP) in Deutschland. Rund 4.000 Unternehmen sorgen für eine flächendeckende Zustellung von der Hallig bis zur Alm, in der Stadt und auf dem Land. Die gesamte Branche realisiert in Deutschland derzeit jährliche Umsätze in Höhe von 27,6 Milliarden Euro, beschäftigt mehr als 260.000 Mitarbeiterinnen und Mitarbeiter und befördert mehr als 4,2 Milliarden Sendungen pro Jahr.