BPEX
BUNDESVERBAND PAKET- UND EXPRESSLOGISTIK

Stellungnahme

Entwurf eines Gesetzes zur Modernisierung und Digitalisierung der Schwarzarbeitsbekämpfung

Aufgrund der komplexen Regelungsmaterie und der knappen Bearbeitungszeit behalten wir uns vor, zu einem späteren Zeitpunkt eine ergänzende Stellungnahme abzugeben.

Der Bundesverband Paket- und Expresslogistik (BPEX) ist die politische Interessenvertretung der Paketbranche in Deutschland. Die Branche liefert flächendeckend täglich ca. 14 Mio. Sendungen an ca. neun Mio. private, gewerbliche und institutionelle Empfängerinnen und Empfänger. Die rund 4.000 Unternehmen der Branche erzielen jährliche Umsätze in Höhe von derzeit 27,6 Mrd. Euro.

Grundsätzlich begrüßt der BPEX das Vorhaben, eine schnellere, effizientere und elektronische Arbeitsweise der Zollbehörden zu ermöglichen. Der BPEX erhebt die Forderung nach einer besseren personellen Ausstattung und mehr Kompetenzen schon seit Jahren.

Nach Anhörung unserer Mitgliedsunternehmen weisen wir dennoch auf die folgenden Bedenken hin.

Erfüllungsaufwand

Als Erfüllungsaufwand für die Wirtschaft wird unter E.2 ein Entlastungsbetrag genannt, den wir für die Branche der Kurier-, Express und Paketdienstleister nicht erkennen können. Nach unserer Auffassung wird eine Kostenbelastung die Folge sein. Um den geforderten Datenzugriff zu ermöglichen, müssen Unternehmen oftmals umfangreiche Programmier- und Anpassungsarbeiten an ihren Systemen durchführen. Anders als bei der Finanzverwaltung sind die konkreten Daten, auf die zugegriffen werden soll, hier nicht eindeutig definiert, während für steuerliche Betriebsprüfungen in ERP-Systemen bereits standardisierte Prüfzugänge vorgesehen sind (z. B. gemäß § 147 Abs. 6 AO). Ein direkter Systemzugriff oder eine umfassende digitale Schnittstellenbereitstellung erfordern erheblichen zeitlichen und organisatorischen Vorlauf sowie umfassende Tests und Sicherheitsbewertungen.

Datenschutz und IT-Sicherheit

Prüfungsumfang nach § 5a Abs. 1 SchwArbG RefE ist unserer Auffassung nach rechtlich unzulässig

§ 5a Abs. 1 SchwArbG RefE sieht eine umfassende elektronische Einsichtnahme in Unterlagen und Daten unmittelbar beim geprüften Unternehmen vor.

Der durch die Prüfbeteiligten zu eröffnende Zugang scheint inhaltlich und über verschiedene Datenverarbeitungssysteme hinweg nicht begrenzt zu sein. Zudem sollen die Daten auch maschinell auf den Systemen des geprüften Unternehmens durch die Finanzkontrolle Schwarzarbeit (FKS) ausgewertet werden können. Ein maßgebliches Kriterium bei der datenschutzrechtlichen Beurteilung ist die Erforderlichkeit. Diese fordern wir auch in diesem Kontext ein. Die zu eröffnenden Zugänge sollten auf ein „erforderliches Maß" beschränkt sein, welches durch den Gesetzgeber zu begründen ist.

Mit den Voraussetzungen des SchwarzArbG RefE werden bei den Prüfbeteiligten zumindest potenziell Risiken geschaffen, da in jedem Fall den Amtsstellen ein zusätzlicher Zugang zur Datenverarbeitung der Prüfbeteiligten geöffnet wird. Zwar gehen wir davon aus, dass die Behörden des Bundes und des Zolls im Besonderen vor unbefugtem Eintritt geschützt sind (wie es in § 4 Abs. 1 ScharzArbG RefE auch als Voraussetzung festgehalten wird), allerdings sind auch erfolgreiche Angriffe wie z. B. auf den Bundestag oder die Bundesbehörden bekannt. Daher sollte jeder zusätzliche Zugang von außen äußerst zurückhaltend bewertet und strikt reguliert werden.

Wir schließen nicht aus, dass die Ausweitung der Befugnisse der Behörden und die korrespondierende Informationspflicht der Behörden den derzeitigen umfassenden Bestrebungen zur Erhöhung des Cybersicherheitsniveaus in der EU zuwider sein könnte. Insbesondere für Unternehmen, die unter den Anwendungsbereich des NIS2UmsG fallen, gibt es eine besondere Problematik: Diese Unternehmen unterliegen strengen Zugangskontrollen (vgl. NIS-2-Richtlinie Art. 21 Abs. 2 Buchst. d)) sowie umfassenden Dokumentationspflichten. Diesen entspricht die Regelung des § 4 Abs. 1 SchwarzArbG RefE (Nutzung des Datenverarbeitungssystems der Prüfungsbeteiligten) oder des § 4 Abs. 1b Nr. 2 SchwarzArbG RefE nicht. Für Unternehmen, die dem NIS2UmsG unterliegen, sollte hier ein Vetorecht vorgesehen werden, wenn der direkte Systemzugriff durch die Zollverwaltung IT-sicherheitsrelevante Aspekte gefährdet oder nicht dem Stand der Technik (z. B. in Bezug auf Zugriffssicherheit und Protokollierung) entspricht. Sicherheitsbedenken der Prüfbeteiligten müssen ausdrücklich berücksichtigt werden.

Akteneinsichtsrecht

Obwohl durch die erweiterten Prüfungsrechte erheblich in die Rechte der Prüfungsbeteiligten eingegriffen wird, wird diesen kein Akteneinsichtsrecht eingeräumt. Ein solches Recht ist jedoch essenziell, um den Grundsatz des rechtlichen Gehörs zu wahren und eine effektive Verteidigung gegenüber behördlichen Maßnahmen zu ermöglichen.

Konflikt mit dem Postgeheimnis

Mit Blick auf weitere Wechselwirkungen im nationalen Recht ist unklar, ob mögliche Konflikte mit dem Postgeheimnis im Rahmen solcher Zugänge bei Unternehmen im Post- und Paketbereich entstehen. In den Systemen der Paketdienste sind zwangsläufig Daten enthalten, die dem Postgeheimnis unterliegen. Dies könnte insbesondere relevant werden,

sollte ein Zugang zu den Systemen mit den Scandaten verlangt werden. Dabei werden von den Zustellerinnen und Zustellern sendungsbezogene Daten (einschließlich Absenderdaten) und Daten der Empfänger (wie z. B. Adressdaten) erfasst. Die Scandaten werden bisher häufig vom Zoll herausverlangt, um Arbeitszeitaufzeichnungen zu prüfen. Bei Übersendung der Daten an den Zoll können die prüfbeteiligten Unternehmen bisher dafür sorgen, dass keine Daten enthalten sind, die dem Postgeheimnis unterliegen.

Mit einem offenen Zugang zum System kann das nicht mehr gewährleistet werden, und es kann zu einem Konflikt mit den spezialgesetzlichen Ermächtigungsgrundlagen zur Weitergabe von Daten in Bezug auf das Postgeheimnis gem. §§ 99, 100 Strafprozessordnung kommen. Zur Anordnung der Weitergabe von Daten, die dem Postgeheimnis unterliegen ist nur das Gericht, bei Gefahr im Verzug auch die Staatsanwaltschaft befugt. Das bedeutet nach unserer Auffassung, dass in der Regel ein richterlicher Beschluss als Voraussetzung von Maßnahmen der Behörden vorliegen muss. Ob und wie Zugänge auf der Nutzungsseite der Behörden mit Blick auf das Postgeheimnis beschränkt werden, ist unklar. Hinzu kommt, dass der IT-Aufwand voraussichtlich immens hoch sein würde, soweit die Systeme überhaupt trennbar sind.

Insgesamt schätzen wir die vorgenommene Ausdehnung des Zugangs für Kontrollen zur Verhinderung und Bekämpfung der Schwarzarbeit als unverhältnismäßig und ungerechtfertigt ein. Wir halten es für ausreichend, wenn vor Ort Prüfungen ermöglicht werden und zur Weiterführung der Ermittlungen entsprechende Dokumente auf Anforderung elektronisch übermittelt werden – ohne automatisierten und umfassenden Zugang. Die extreme Erweiterung der Befugnis ist aus rechtsstaatlicher Sicht abzulehnen.

Verstoß gegen datenschutzrechtliche Prinzipien bei § 5 Abs. 5 SchwArbG RefE – Grundsatz der Datenminimierung

§ 5 Abs. 5 SchwArbG RefE sieht vor, dass Prüfbeteiligte automatisiert verarbeitbare Datenträger oder Daten „ungesondert" zur Verfügung stellen dürfen, wenn die Aussonderung mit unverhältnismäßigem Aufwand verbunden wäre und überwiegende schutzwürdige Interessen der betroffenen Personen nicht entgegenstehen.

Es müsste aus unserer Sicht ein Interesse daran bestehen, die Unternehmen und deren Aufwand für einen datenschutzrechtlich richtigen Umgang mit Daten zu schützen. Dies erfordert aus unserer Sicht, dass nicht eine dritte Stelle beurteilt, ob ein unverhältnismäßig hoher Aufwand für die Absonderung von nicht erforderlichen Daten besteht, sondern dass die Pflicht der Behörden der Zollverwaltung nach § 5 Abs. 5 Satz 2 SchwArbG RefE unmittelbar und in jedem Fall greift. Zudem kommt es unserer Auffassung nach nicht darauf an, ob ein Aufwand verhältnismäßig oder unverhältnismäßig hoch ist, sondern darauf, ob er „erforderlich" ist. Damit würde die Regelung den EU-rechtlichen Vorgaben gerecht werden, die sich auch im § 47 Nr. 3 Bundesdatenschutzgesetz widerspiegeln. Dieser sieht vor, dass personenbezogene Daten dem Verarbeitungszweck entsprechen müssen, für das Erreichen des Verarbeitungszwecks erforderlich sein müssen und ihre Verarbeitung nicht außer Verhältnis zu diesen Zwecken stehen darf.

Die derzeit gewählte Formulierung begrenzt die Datenverarbeitung nicht auf das erforderliche Maß und begegnet grundlegenden datenschutzrechtlichen Bedenken.

§ 15 SchwArbG RefE enthält einen unklaren Begriff der „Erforderlichkeit"

Es bestehen auch datenschutzrechtliche Bedenken gegen die Vorgaben zur Datenverarbeitung im Hinblick auf den Grundsatz der Datenminimierung und die Begrenzung auf die Erforderlichkeit in § 15 Abs. 2 SchwArbG RefE. Hier geht es insbesondere darum, dass durch das Adjektiv „unbeschadet" nicht klar genug wird, wann die in § 15 Abs. 1 genannten Regelungen der Strafprozessordnung und des Gesetzes über Ordnungswidrigkeiten weiterhin greifen. Wir halten eine Klarstellung für nötig, ob in jedem Fall der Anwendung von § 15 Abs. 2 Nr. 2 die Strafprozessordnung bei Verarbeitung personenbezogener Daten im Ermittlungsverfahren ausgesetzt werden soll oder nicht.

„Risikoorientierter Ansatz" (§ 25 Abs. 2 SchwArbG RefE) zu unklar - Raum für Vorverurteilung

Der Referentenentwurf sieht einen neuen „risikoorientierten Ansatz" der FKS insbesondere für die Auswahl der zu prüfenden Unternehmen vor. Die Risikobewertung und Auswahl sind unklar und letztlich eine Blackbox. Es gibt die Befürchtung, dass nicht sachlich fundierte, sondern medial präsente Faktoren Einfluss auf die Risikobewertung nehmen könnten. Wenn in der Folge die „üblichen Verdächtigen" im Fokus stehen, wäre eine Konsequenz zumindest eine mögliche falsche Schwerpunktsetzung, die die Effizienz der Bekämpfung von Schwarzarbeit in anderen Branchen senken kann.

Vorrangig sollen diejenigen geprüft werden, bei denen ein höheres Risiko für das Auftreten von Schwarzarbeit und illegaler Beschäftigung besteht. § 25 Abs. 2 SchwArbG RefE zeigt aber, dass die genannten Risikoindikatoren letztlich erheblichen Interpretationsspielraum lassen („Anomalien im Zusammenhang mit…").

Wenngleich wir begrüßen, dass zumindest nachgelagert an das zentrale Informationssystem übermittelte Risikohinweise einschließlich derjenigen Risikoindikatoren, die zu einem Risikohinweis geführt haben, einer datenschutzrechtlichen Überprüfung zugänglich sein müssen, bleibt doch festzuhalten, dass es sich dabei immer nur um eine nachträgliche Kontrolle handelt.

Erweiterung der Befugnisse und Mitwirkungspflichten

Der Referentenentwurf führt zu einer erheblichen Erweiterung der Befugnisse der Behörden bei der Prüfung von Unterlagen nach § 4 SchwarzArbG RefE. Damit verbunden ist ein umfassender Zugang zu den Datenverarbeitungssystemen der Prüfbeteiligten durch Dritte, was vor dem Hintergrund der Diskussion um Datensicherheit grundsätzlich kritisch zu würdigen ist. Mit der Ausweitung des Prüfzugangs werden auch die Mitwirkungspflichten der Prüfbeteiligten ausgeweitet, ohne dass deren Reichweite und Umfang immer ganz klar

ist. So sind Prüfbeteiligte nach § 5a Abs. 2 ScharwArbG RefE verpflichtet, bei der Datenweitergabe ein maschinell lesbares Format nach den Vorgaben der Behörden zu verwenden.

Im Fall einer Aktualisierung von Datenformaten bei den Unternehmen schwingt immer mit, dass die Unternehmen sicherstellen müssen, dass die Daten im Zweifel in alten Datenformaten vorgehalten werden müssen, um der Anforderung der Lesbarkeit durch die Zollbehörden zu genügen. Aus unserer Sicht angemessener wäre eine Pflicht der Zollbehörden, stets auf dem aktuellen Stand der Technik zu sein.

Einwilligung bei Sozialdaten

Gemäß § 5a Abs. 2 SchwarzArbG RefE soll der Prüfungsbeteiligte bei Sozialdaten eine Einwilligung vorlegen. Die Übermittlung von Sozialdaten ist jedoch in § 69 SGB X sehr restriktiv geregelt.

Es bleibt unklar, ob sich die verlangte Einwilligung auf die einzelnen Arbeitnehmer bezieht und ob diese jeweils individuell einzuholen ist, z. B. im Rahmen der Lohn- und Gehaltsabrechnung. Diese Unklarheit zeigt, dass der Gesetzgeber selbst davon ausgeht, dass die rein gesetzliche Grundlage für die Herausgabe der Daten nicht ausreichend ist. Des Weiteren stellt sich die Frage, ob bei einer gescheiterten Abstimmung immer das Einwilligungsprinzip gelten soll.

Sanktionen von Verstößen angemessen halten und Rechtssicherheit erhöhen

Ergänzend werden Sanktionen bei Ordnungswidrigkeiten ausgeweitet. In § 21 Abs. 1 Satz 1 Nr. 1 SchwArbG RefE wird neu auf § 8 Abs. 3 SchwArbG RefE verwiesen. Damit würde die Ordnungswidrigkeit der leichtfertigen (fahrlässigen) Vorenthaltung von Sozialversicherungsbeiträgen künftig auch das Risiko begründen, von öffentlichen Aufträgen ausgeschlossen zu werden, was eine erhebliche Verschärfung darstellen würde.

Prüfung von Personen

An mehreren Stellen – insbesondere in § 3 Abs. 1a Nr. 1 und § 5 Abs. 1 Nr. 3a SchwArbG RefE – ist vorgesehen, dass Auskünfte gegebenenfalls „an Amtsstelle mündlich" zu erteilen sind. Zur Klarheit und damit auch zur Akzeptanz der Regelung würde sicherlich beitragen, wenn die Formulierung der Begründung Eingang in den Regelungstext finden würde. In der Begründung heißt es zu § 3 Abs. 1a Nr. 1: „Der Prüfungsort sowie die Art der Übermittlung bzw. Einsichtnahme wird von den Bediensteten der FKS einzelfallbezogen im Rahmen ihrer Ermessensausübung und unter Beachtung des Verhältnismäßigkeitsgrundsatzes festgelegt". Die Aufnahme des Verhältnismäßigkeitsgrundsatzes würde nach unserer Auffassung ein abgestuftes Abwägungsverfahren beinhalten, das besonders dem Kriterium der Erforderlichkeit gerecht wird.

Übergangsfristen

Insofern, als dass die neuen Anforderungen umfassende Änderungen an den IT-Systemen erfordern (Übermittlungspflichten, Zugänge etc.), ist es zwingend erforderlich, ausreichende Übergangsfristen vorzusehen. Die Regelung in Art. 18 SchwArbG RefE enthält gerade keine Übergangsfrist. Das können die Unternehmen nicht leisten.

Aus dem Kreis der Mitgliedsunternehmen haben wir erfahren, dass im Rahmen von Zollprüfungen bisher nur ein Hauptzollamt einen geschützten Upload-Bereich zur Verfügung stellt. Ein direkter Systemzugriff oder eine umfassende digitale Schnittstellenbereitstellung erfordern erheblichen zeitlichen und organisatorischen Vorlauf sowie umfassende Tests und Sicherheitsbewertungen.

Berlin, im Juli 2025