

ZOLLRECHT

AKTUELL

Ihr starker Partner für die tägliche Zollabwicklung

KW 26 | 2025



3 Nutzen Sie die Vorteile des neuen Freihandelsabkommens Moldau – EFTA

Neues Freihandelsabkommen zwischen Moldau und der EFTA: Sichern Sie sich die Wettbewerbsvorteile

4 Neue vorläufige Antidumpingzollsätze für bestimmte Produkte

Antidumpingzölle auf Kettenplatten aus Stahl mit Ursprung in China – Diese Warentarifnummern sind davon betroffen

TOP-THEMA

5 Cyberbedrohungen – Angriffe nehmen weiter zu

Cybersicherheit im Zoll- und Außenwirtschaftsbereich der EU: Schützen Sie Ihr Unternehmen

10 Richtige Kontrolle der Einfuhrsteuerbescheide – So geht's

Verhindern Sie Bußgeldverfahren – Prüfen Sie Ihre Steuerbescheide

EDITORIAL**Julianna Straib-Lorenz**

ist Unternehmensberaterin. Mit mehr als 16 Jahren Erfahrung im operativen Zoll- und Logistikbereich, Beratung von Firmen und Schulung dieser.

Global handeln, lokal prüfen – der Ursprung zählt!

Liebe Leserin, lieber Leser,

weltweit schießen Freihandelsabkommen derzeit schneller aus dem Boden als Ihre Lieblingspflanze im Frühling. Die Vereinigten Arabischen Emirate schließen reihenweise CEPA-Abkommen ab – zuletzt mit Costa Rica und Mauritius. Was nach sonnigen Urlaubszielen klingt, ist für Sie als international tätiges Unternehmen vor allem eins: eine Einladung zum Zollsparen.

Doch aufgepasst: Mit jedem neuen Abkommen steigt auch die Bedeutung sauberer Ursprungsprüfungen. Denn Zollfreiheit gibt es nicht umsonst – sie will verdient sein und vor allem nachgewiesen. Und das bedeutet: Präferenzkalkulation, Ursprungsnachweise und der liebevolle Blick in die Lieferkette. Ein falscher Präferenznachweis kann da mehr Kopfzerbrechen bereiten als der Versuch, eine Ananas mit Zolldtarifnummer zu versehen.

Also, behalten Sie Ihre Ursprungskriterien im Blick – am besten bevor die Ware unterwegs ist. Denn im globalen Handel gilt: Wer richtig nachweist, spart richtig ein. Und wir helfen Ihnen dabei.

Herzlichst Ihre

Julianna Straib-Lorenz,
Chefredakteurin

INHALTSVERZEICHNIS**NEWS 3**

- ☐ Neues Freihandelsabkommen zwischen Moldau und der EFTA: Das sollten Sie jetzt wissen
- ☐ Antidumpingzölle auf Kettenplatten aus Stahl mit Ursprung in China

NEWS 4

- ☐ Ecuador senkt Importzölle auf bestimmte US-Produkte

TOP-THEMA 5

- ☐ Cybersicherheit im Zoll- und Außenwirtschaftsbereich der EU: Schützen Sie Ihr Unternehmen

ARBEITSHILFE 8

- ☐ Checkliste – Prüfen Sie den Stand Ihrer IT-Sicherheit

LESERFRAGEN 9

- ☐ Muss ich meine Präferenznachweise jetzt wieder im Original vorliegen haben?
- ☐ Kann ich auch eine Rückware anmelden, wenn sie nicht vom damaligen Kunden zurückkommt?

GASTBEITRAG 10

- ☐ Verhindern Sie Bußgeldverfahren – Prüfen Sie Ihre Steuerbescheide auf Richtigkeit

KURZMELDUNGEN 12

- ☐ Zollanmeldung – Mit unserer Arbeitshilfe prüfen Sie diese immer korrekt!
- ☐ Neue Handelsabkommen der VAE mit Costa Rica und Mauritius in Kraft

Hier können Sie den Text abhaken, wenn Sie ihn fertig durchgearbeitet haben.



Alle Arbeitshilfen als Downloads unter
www.zolex.de/arbeitshilfen

NEWS

Neues Freihandelsabkommen zwischen Moldau und der EFTA: Sichern Sie sich diese Wettbewerbsvorteile

Am 1. April 2025 ist das Freihandelsabkommen (FHA) zwischen der Republik Moldau und den Mitgliedstaaten der Europäischen Freihandelsassoziation (EFTA) in Kraft getreten. Die EFTA-Staaten – Island, Liechtenstein, Norwegen und die Schweiz – schaffen damit neue Perspektiven für den grenzüberschreitenden Handel mit einem aufstrebenden osteuropäischen Partner.

Was bringt Ihnen das Abkommen konkret?

Für Sie als exportierendes oder importierendes Unternehmen bedeutet das Abkommen in erster Linie eins: Zollvorteile. Künftig werden 98,5 Prozent aller Waren, die aus EFTA-Staaten nach Moldau exportiert werden, zollfrei eingeführt. Das reduziert Ihre Kosten und verbessert Ihre Wettbewerbsfähigkeit. Aber das Abkommen geht weit über Zollfragen hinaus. Es schafft klare Regeln für:

- 🌐 Investitionen
- 🌐 Schutz geistigen Eigentums
- 🌐 Abbau nicht tarifärer Handelshemmnisse
- 🌐 Wettbewerbsregeln
- 🌐 Handelserleichterungen
- 🌐 Nachhaltigkeitsaspekte

Ein besonderes Highlight: Zum ersten Mal gelten im Rahmen eines EFTA-Abkommens auch umfassende Regelungen zum elektronischen Handel. Damit trägt das Abkommen aktuellen wirtschaftlichen Entwicklungen Rechnung und bietet Ihnen als digital aufgestelltem Unternehmen mehr Rechtssicherheit.

Warum ist das politisch relevant?

Angesichts des russischen Angriffskriegs gegen die Ukraine und der geopolitischen Lage in Osteuropa ist das Abkommen nicht nur ökonomisch, sondern auch politisch ein starkes Signal. Es

stärkt die wirtschaftliche Zusammenarbeit zwischen der EFTA und einem Staat, der sich klar europäisch orientiert.

Was sollten Sie jetzt tun?

Wenn Sie Waren nach Moldau exportieren oder von dort beziehen, prüfen Sie jetzt Ihre Lieferketten:

- 🌐 Können Sie von der Zollfreiheit profitieren?
- 🌐 Erfüllt Ihre Ware die Voraussetzungen für eine Präferenzbehandlung?
- 🌐 Ist Ihre Dokumentation für den Ursprungsnachweis auf dem aktuellen Stand?

Auch wenn Sie im digitalen Handel aktiv sind, lohnt sich ein Blick in die neuen Bestimmungen – insbesondere zu Datentransfer, Verbraucherschutz und elektronischen Vertragsabschlüssen.



FAZIT

Das neue Freihandelsabkommen bietet Ihnen zahlreiche Chancen – von niedrigeren Zöllen bis hin zu stabileren rechtlichen Rahmenbedingungen. Nutzen Sie die Gelegenheit, um Ihre Geschäftsbeziehungen mit Moldau auf ein neues Niveau zu heben.

Autorin: Julianna Straib-Lorenz

Antidumpingzölle auf Kettenplatten aus Stahl mit Ursprung in China – Sind Sie betroffen?

Die Europäische Kommission hat mit Wirkung zum 23. April 2025 vorläufige Antidumpingzölle auf bestimmte Kettenplatten aus Stahl festgelegt, die aus China in die EU eingeführt werden. Das entsprechende Antidumpingverfahren wurde bereits im August 2024 eingeleitet. Prüfen Sie, inwieweit Sie davon betroffen sind.

Die Maßnahmen betreffen Einfuhren von

- 🌐 bestimmten Stahlplatten, ggf. mit Gummiauflagen,
- 🌐 ggf. zu einer Laufkette zusammengesetzt,

- 🌐 mit einer Länge von höchstens 3.000 mm,

- 🌐 verwendet für Maschinen der KN-Positionen 8426, 8429 oder 8430 oder für Förderbänder der Position 8428.

Die Einreihung erfolgt unter folgenden KN-/TARIC-Codes:

- 🌐 ex 8431 39 00, ex 8431 49 20, ex 8431 49 80
- 🌐 TARIC-Codes: 8431 39 00 21, 25, 26, 29 / 8431 49 20 11, 15, 16, 19 / 8431 49 80 11, 15, 16, 19

Wie hoch ist der vorläufige Antidumpingzoll auf die betreffenden Waren?

Der vorläufige Antidumpingzollsatz beträgt:

- 🌐 62,5 % auf den Nettopreis frei Grenze der Union, unverzollt
- 🌐 55 % des Nettopreises für Laufkettenbaugruppen
- 🌐 50 % für vollständige Laufkettenbaugruppen

Um die Ware in den zollrechtlich freien Verkehr überführen zu können, muss eine Sicherheit in Höhe des vorläufigen Zolls geleistet werden.

Wie geht es weiter?

Die Kommission hat nun Zeit bis Oktober 2025, um die Untersuchung abzuschließen. Danach können endgültige Antidumpingzölle festgelegt werden – diese können höher, niedriger oder identisch mit den vorläufigen Zöllen ausfallen.



ACHTUNG

Seit Oktober 2024 werden die betroffenen Waren zollamtlich erfasst. Das bedeutet: Eine rückwirkende Anwendung der endgültigen Antidumpingzölle ist möglich, sofern die Kommission dies in ihrer Endentscheidung vorsieht.

Was sollten Sie tun?

- 🌐 Prüfen Sie, ob Ihre Produkte unter die betroffenen TARIC-Codes fallen.
- 🌐 Kalkulieren Sie die möglichen Antidumpingzölle in Ihre Preisgestaltung ein.
- 🌐 Stellen Sie sicher, dass Ihre Zollanmeldungen korrekt und vollständig sind.
- 🌐 Behalten Sie die Entwicklung der endgültigen Entscheidung im Blick, insbesondere im Hinblick auf eine mögliche Rückwirkung.

Bei Unsicherheiten sollten Sie rechtzeitig zollrechtliche Beratung einholen.

Autorin: Julianna Straib-Lorenz

Ecuador senkt Importzölle auf bestimmte US-Produkte

Ecuador hat als Reaktion auf geplante US-Zusatzzölle auf ecuadorianische Waren Gegenmaßnahmen beschlossen, die zugleich die wirtschaftliche Zusammenarbeit mit den Vereinigten Staaten stärken sollen.

Zollsenkung auf US-Leichtfahrzeuge

Der ecuadorianische Außenhandelsausschuss (COMEX) hat mit Resolution Nr. 003-2025 beschlossen, die Einfuhrzölle auf bestimmte Leichtfahrzeuge aus den USA auf 10 % zu senken. Diese Maßnahme gilt seit dem 10. April 2025 und ist bis zum 31. Dezember 2025 befristet. Wichtig: Damit Sie vom ermäßigten Zollsatz profitieren, müssen folgende Voraussetzungen erfüllt sein:

- 🌐 Die Waren müssen mit einem Ursprungszeugnis der USA eingeführt werden und die betroffenen Zolltarifnummern sind in der Resolution auf Seite 9 aufgeführt.

Zollsenkung auf Garnelenprodukte

Bereits zuvor hatte COMEX mit Resolution Nr. 002-2025 beschlossen, die Importzölle auf bestimmte Garnelenprodukte auf 0 % zu senken. Diese Maßnahme trat am 29. März 2025 in Kraft und gilt ebenfalls bis zum 31. Dezember 2025.

Folgende Zolltarifnummern sind betroffen:

0306.17, 0306.17.11.00, 0306.17.12.00, 0306.17.13.00, 0306.17.14.00, 0306.17.19.00, 0306.17.91.00, 0306.17.99, 0306.17.99.10, 0306.17.99.20, 0306.17.99.90

Autorin: Julianna Straib-Lorenz

TOP-THEMA

Cybersicherheit im Zoll- und Außenwirtschaftsbereich der EU: So schützen Sie Ihr Unternehmen

Die Digitalisierung macht auch vor dem Zoll- und Außenwirtschaftsbereich nicht halt. Elektronische Zollabfertigungssysteme, automatisierte Prozesse und global vernetzte Lieferketten bringen zweifellos Effizienzgewinne – aber sie vergrößern gleichzeitig auch die Angriffsfläche für Cyberkriminelle. Gerade die IT-Systeme von Zollbehörden und international tätigen Unternehmen verarbeiten hochsensible Handelsdaten und sind damit ein attraktives Ziel. Als Unternehmen im Außenhandel sollten Sie die Bedrohungslage daher ernst nehmen und präventiv handeln.



Typische Cyberangriffe im Zollumfeld – und wie Sie sich und Ihr Unternehmen am besten schützen

Tatsächlich richteten sich allein 2023/24 rund 19 % aller Cyberangriffe in Europa gegen Einrichtungen der öffentlichen Verwaltung – also auch gegen Zollbehörden. Weitere 11 % betrafen den Transport- und Logistiksektor. Doch wie können solche Angriffe aussehen? Und vor allem, wie können Sie solche Angriffe abwehren? Nachfolgend erhalten Sie einen detaillierten Überblick.

Phishing & Social Engineering

Angreifer versuchen, Ihre Mitarbeitenden durch gefälschte E-Mails oder SMS zur Preisgabe von Zugangsdaten zu verleiten. Typisch sind z. B. E-Mails von "zoll@dhl.de" oder "noreply@zoll.de", die angebliche Zollgebühren einfordern. Besonders perfide: Spear-Phishing, das gezielt Zollmitarbeitende oder Außenhandelsexperten ins Visier nimmt.



MEIN TIPP

Es kommt vor allem immer häufiger vor, dass Sie als Mitarbeiter eine E-Mail erhalten und einfach draufklicken. Wenn Ihnen die Absenderadresse unbekannt ist oder Namen und Zeichen enthält, die teilweise kryptisch wirken, dann senden Sie diese Mail an Ihre IT weiter, um sie überprüfen zu lassen, BEVOR Sie auf den Link klicken. Schon ein einziger Klick kann ausreichen, um Schadsoftware ins System zu schleusen oder sensible Daten preiszugeben. Gerade in exportkontrollrechtlich sensiblen Unternehmen kann dies auch sicherheitsrelevante Folgen haben.

Ihre Schutzmaßnahmen:

- 🌐 Mitarbeiterschulungen zur Erkennung von Phishing
- 🌐 Technische Filter für verdächtige E-Mails
- 🌐 Einsatz von Mehr-Faktor-Authentifizierung (MFA)

Ransomware (Erpressungssoftware)

Diese Angriffe verschlüsseln Ihre Systeme, nachdem zuvor oft Daten gestohlen wurden. Besonders riskant für Logistikunternehmen: Ein Ransomware-Angriff kann den Warenfluss komplett lahmlegen – wie etwa beim Logistiker Hellmann oder der Reederei Maersk.

Ihre Schutzmaßnahmen:

- 🌐 Regelmäßige Backups und Notfallpläne
- 🌐 Schwachstellenmanagement und Patch-Management
- 🌐 Zugriffsschutz für externe Verbindungen (z. B. VPN nur mit MFA)

Supply-Chain-Angriffe

Angreifer infiltrieren gezielt Dienstleister oder Softwareanbieter in Ihrer Lieferkette. Beispiel: Im Hafen von Antwerpen nutzten Schmuggler über Jahre hinweg manipulierte Zugangsdaten, um Container mit Schmuggelware verschwinden zu lassen. Auch in der Schweiz wurde im Jahr 2023 ein externer IT-Dienstleister gehackt, wodurch sensible Zoll Daten im Darknet landeten.

Ihre Schutzmaßnahmen:

- 🌐 Sicherheitsanforderungen vertraglich an Ihre Partner binden
- 🌐 Prüfung von Software-Updates und Zugriffen von Drittanbietern
- 🌐 Monitoring und Segmentierung der Netzwerke

Insider-Bedrohungen

Nicht nur externe Hacker sind ein Risiko. Auch Mitarbeitende oder Partner mit Zugriffsrechten können absichtlich oder fahrlässig Schaden anrichten. Besonders kritisch: physische Zugänge in Logistikzentren oder Serverräumen.

Ihre Schutzmaßnahmen:

- 🌐 Zugriffsrechte nach dem Minimalprinzip vergeben
- 🌐 Vier-Augen-Prinzip bei kritischen Aktionen
- 🌐 Videoüberwachung und Zutrittskontrollen

Das sind die aktuellen Entwicklungen und Trends in der EU

Betrachten wir innerhalb der EU die Entwicklungen, dann kann gesagt werden, dass die Angriffe auf Unternehmen zunehmen. Das bedeutet, Sie müssen noch mehr Vorsicht walten lassen.

Zunahme von Ransomware und Erpressungsfällen

Ransomware-Angriffe nehmen europaweit weiter zu – und sie betreffen zunehmend auch den Zoll- und Logistiksektor. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) haben sich Umfang und Raffinesse dieser Angriffe stark erhöht. Täter stehlen häufig zunächst sensible Handels- oder Kundendaten, bevor sie die Systeme verschlüsseln. Im Jahr 2023 lag die Gesamtsumme gezahlter Lösegelder in Europa erstmals über einer Milliarde Euro. Hinzu kommen indirekte Kosten wie Betriebsunterbrechungen, Vertragsstrafen und Imageschäden. Besonders gefährdet sind kritische Dienstleister, deren Ausfall ganze Lieferketten blockieren kann.

Gezielte Angriffe auf Lieferketten und Dienstleister

Ein wachsender Trend sind Angriffe auf vorgelagerte Dienstleister, etwa durch kompromittierte Software-Updates oder gezielte Hacks von Cloud-Anbietern. Das zeigt unter anderem der Angriff auf den Schweizer Softwareanbieter Xplain, bei dem Zoll Daten in falsche Hände gerieten. Die EU-Agentur ENISA warnt, dass solche Supply-Chain-Angriffe bis 2030 zu den größten Bedrohungen zählen könnten. Besonders im Fokus stehen IT-Systeme von Speditionen, Tracking-Plattformen und Logistikzulieferern.



ACHTUNG

Gehören Sie zu den oben genannten Anbietern, dann prüfen Sie gezielt, inwieweit Ihre IT-Sicherheit gewährleistet ist. Dabei geht es vor allem auch um Fremd-Hardware, wie z. B. USB-Sticks oder firmenfremde Handys, die an das Netzwerk angeschlossen werden. Bauen Sie dazu Sicherheitsmaßnahmen ein bzw. verbieten Sie dies gänzlich. Denn schon ein infiziertes Gerät kann ausreichen, um Zugriff auf sensible Exportdaten oder interne Prozesse zu ermöglichen.

Staatliche und „haktivistische“ Cyberangriffe nehmen zu

Neben kriminellen Gruppen treten auch staatlich gesteuerte Angreifer und ideologisch motivierte Haktivisten stärker in Erscheinung. So legten etwa prorussische Gruppen im Januar 2023 die Website der finnischen Zollbehörde per DDoS-Angriff lahm. In der Schweiz mussten im Jahr 2024 verschiedene Zollsyste zeitweise in den Notbetrieb übergehen. Auch sogenannte APT-Gruppen führen gezielte Spionageangriffe durch, um wirtschaftlich relevante Daten (z. B. zu Exporten oder Sanktionsumgehungen) abzugreifen. Für Zollbehörden und international tätige Unternehmen bedeutet dies: Sie müssen mit einer doppelt anspruchsvollen Bedrohungslage rechnen.

Behördliche Warnungen und rechtliche Konsequenzen

Die EU-Kommission und ENISA fordern mehr Wachsamkeit und systematisches Risikomanagement. Nationale Stellen wie das BSI oder Frankreichs ANSSI geben regelmäßig branchenspezifische Warnhinweise. Auch die deutsche Zollverwaltung reagiert – etwa im Juli 2024 mit einer Stellungnahme zu angeblichen Datenlecks im ATLAS-System. EU-weit wurde zudem ein Cyber-Sanktionsregime etabliert, mit dem Angreifer aus dem Ausland sanktioniert werden können. Die Botschaft ist eindeutig: Cybersicherheit hat im Außenwirtschaftsbereich oberste Priorität.

Diese besonderen Herausforderungen für Zollbehörden und außenwirtschaftliche Unternehmen bestehen

Hohe Komplexität und Integration der Systeme

Zollprozesse sind heute paneuropäisch vernetzt und in globale Lieferketten eingebunden. Diese IT-Vernetzung ist operativ notwendig, eröffnet aber auch zahlreiche Angriffspunkte. Sicherheitslücken bei einem Partner können sich schnell auf alle Systeme auswirken. Viele Behörden nutzen zudem veraltete IT-Systeme, die modernisiert werden müssen. Die geplante EU-Zollreform mit einer einheitlichen digitalen Plattform bietet Chancen – aber auch neue Sicherheitsfragen.

Attraktivität als Ziel für Kriminelle und Staatsspieler

Zoll- und Handelsdaten sind von hohem Wert – für Schmuggler wie für staatliche Akteure. Organisierte Kriminelle nutzen Cyberangriffe zur Umgehung von Kontrollen. Staatliche Gruppen interessieren sich für sensible Exportdaten, Dual-Use-Güter oder Sanktionsverstöße. Die Vielfalt der Angreifer verlangt eine ebenso vielseitige Abwehrstrategie.

Veraltete Technologien und ungesicherte Prozesse in der Logistikkette

Viele Lager- und Zollsyste arbeiten mit spezieller Software, die selten aktualisiert wird. Teilweise kommen Geräte zum Einsatz, die sich nicht einfach patchen lassen. Schwachstellen entstehen durch fehlende Netztrennung oder zu enge IT-Integration zwischen Partnern ohne einheitliche Sicherheitsstandards. Angreifer

können sich so unbemerkt von einem Unternehmen zum nächsten bewegen.

Menschlicher Faktor und Fachkräftemangel

Viele Sicherheitsvorfälle entstehen durch menschliches Fehlverhalten – etwa durch Phishing oder unsichere Passwörter. Gleichzeitig fehlt es an IT-Sicherheitspersonal. Behörden und mittelständische Unternehmen konkurrieren mit der Privatwirtschaft um Fachkräfte. Oft bleibt die Cybersicherheit „nebenbei“ an überlasteten IT-Teams hängen.

Regulatorische und organisatorische Anforderungen

Neue Vorgaben wie die NIS2-Richtlinie oder die Datenschutz-Grundverordnung erhöhen die Anforderungen. Für viele kleinere Unternehmen bedeutet dies einen erheblichen Aufwand – technisch, organisatorisch und finanziell. Ohne passende Unterstützung können einzelne Akteure zum Sicherheitsrisiko für die gesamte Lieferkette werden.

Diese Best Practices für Ihre Cybersicherheit im Zoll- und Außenwirtschaftsbereich helfen Ihnen weiter

Cyberangriffe auf den Zoll- und Außenwirtschaftsbereich nehmen stetig zu. Um sich wirksam zu schützen, brauchen Sie mehr als nur Antivirensoftware und eine Firewall. Hier erfahren Sie, welche Best Practices sich bewährt haben und wie Sie Ihr Unternehmen widerstandsfähiger machen.

1. Erfüllen Sie die gesetzlichen Sicherheitsstandards
Die EU verpflichtet Unternehmen mit der NIS2-Richtlinie zu einem Mindestniveau an Cybersicherheit. Dazu gehören Risikoanalysen, technische und organisatorische Schutzmaßnahmen, Vorfallmeldungen und ein klar benannter Sicherheitsverantwortlicher. Prüfen Sie, ob und in wieweit Ihr Unternehmen diese Vorgaben erfüllt. Nutzen Sie anerkannte Standards wie ISO/IEC 27001 oder den BSI-Grundschutz, um Ihre Sicherheitsprozesse strukturiert aufzubauen. Auch nationale Vorgaben wie das IT-Sicherheitsgesetz müssen eingehalten werden.
2. Setzen Sie auf moderne IT-Sicherheitsarchitekturen
Schützen Sie Ihre Infrastruktur konsequent:
Netzwerksegmentierung: Trennen Sie kritische Systeme von allgemeinen Büro-Netzen.
3. Patchmanagement: Aktualisieren Sie Software und Betriebssysteme regelmäßig.
4. Zugriffskontrollen: Arbeiten Sie nach dem Prinzip der minimalen Rechte, nutzen Sie MFA.
5. Datenverschlüsselung und Backups: Schützen Sie Daten bei Übertragung und Speicherung. Backups sollten offline bzw. unveränderlich gesichert sein.
6. Notfallplanung: Legen Sie fest, wie Sie bei einem Cyberangriff reagieren und Systeme wiederherstellen.
7. Behalten Sie Ihre Lieferkette im Blick
Viele Angriffe kommen über Partner. Sorgen Sie deshalb für ein strukturiertes Cyber Supply Chain Risk Management: Erfassen und bewerten Sie alle IT-Dienstleister und Speditionspartner.
8. Legen Sie Sicherheitsanforderungen vertraglich fest (z. B. Updates, Authentifizierung).
9. Führen Sie regelmäßig Audits durch oder lassen Sie sich Zertifikate (z. B. ISO 27001) vorlegen.
10. Beobachten Sie Sicherheitsvorfälle bei Partnern aktiv (z. B. über CERT-Meldungen).
11. Schulen Sie Ihre Mitarbeitenden
Menschen sind oft das schwächste Glied in der Sicherheitskette. Sensibilisieren Sie Ihr Team: Regelmäßige Schulungen zu Cybergefahren und sicherem Verhalten
12. Interne Phishing-Tests zur Überprüfung des Sicherheitsbewusstseins
13. Klare Meldewege für verdächtige Vorfälle
14. Kampagnen und Poster zur Stärkung der Sicherheitskultur
15. Etablieren Sie ein effektives Incident Response Management
Angriffe lassen sich nicht immer verhindern, aber gut abwehren: Betreiben Sie Monitoring (z. B. Log-Analyse, Intrusion Detection)
16. Halten Sie einen Notfallplan bereit: Wer tut was im Ernstfall?
17. Üben Sie den Ernstfall regelmäßig in Form von Cyber-Drills oder Penetrationstests.
18. Kooperieren Sie mit anderen Stellen. Cybersicherheit ist Teamarbeit. Nutzen Sie Informationsnetzwerke wie: CSIRTs und CERTs
19. Austausch mit Zollbehörden und Strafverfolgung
Melden Sie Vorfälle aktiv weiter, um andere zu warnen. So entsteht kollektive Sicherheit.
20. Denken Sie auch an Organisation und Strategie. Cybersicherheit braucht Rückenwind von oben: Verankern Sie IT-Sicherheit in Ihrer Unternehmensstrategie.
21. Denken Sie auch an physische Sicherheit (Zutritt, Videoüberwachung etc.).
22. Prüfen Sie Cyber-Versicherungen als Teil Ihres Risikomanagements.



FAZIT

Cyberbedrohungen im Zoll- und Außenwirtschaftsbereich sind real und nehmen stetig zu. Doch mit einem ganzheitlichen Sicherheitskonzept, regelmäßigen Schulungen, technischen Schutzmaßnahmen und klaren Verantwortlichkeiten können Sie Ihr Unternehmen wirksam schützen. Denken Sie daran: Jede digitale Zollanbindung ist nur so sicher wie ihr schwächster Punkt.

Autorin: Julianna Straib-Lorenz



Checkliste – Prüfen Sie den Stand Ihrer IT-Sicherheit

Nutzen Sie diese Checkliste, um zu prüfen, wie gut Sie im Bereich Cybersicherheit aufgestellt sind.

 CHECKLISTE CYBERSICHERHEIT (ZOLL UND AUSSENWIRTSCHAFT) 		
Frage	Ja	Nein
Haben Sie einen oder mehrere Verantwortliche für Cybersicherheit benannt?	☐	☐
Führen Sie regelmäßig Risikoanalysen Ihrer IT-Systeme durch?	☐	☐
Erfüllen Sie alle Meldepflichten für erhebliche Sicherheitsvorfälle?	☐	☐
Orientieren Sie sich an etablierten Standards wie ISO/IEC 27001 oder dem BSI-Grundschutz?	☐	☐
Haben Sie Ihre Netzwerke in Zonen unterteilt (z. B. Trennung zwischen Büro- und Logistiksystemen)?	☐	☐
Nutzen Sie Firewall-Zonen und DMZ zur Abschottung sensibler Systeme?	☐	☐
Patchen Sie Ihre Systeme regelmäßig und zeitnah nach Veröffentlichung sicherheitsrelevanter Updates?	☐	☐
Haben Sie einen Prozess zum Umgang mit nicht patchbaren Systemen (z. B. Virtual Patching)?	☐	☐
Verwenden Sie durchgängig Multi-Faktor-Authentifizierung (MFA) für externe und kritische Zugänge?	☐	☐
Ist das Prinzip der minimalen Rechte (Least Privilege) konsequent umgesetzt?	☐	☐
Verschlüsseln Sie Ihre Daten sowohl im Ruhezustand als auch während der Übertragung?	☐	☐
Sind regelmäßige, offline gespeicherte Backups vorhanden und getestet?	☐	☐
Haben Sie einen funktionierenden Incident Response Plan inklusive Notfallprozessen?	☐	☐
Führen Sie regelmäßige Cyber-Drills oder Penetrationstests durch?	☐	☐
Haben Sie eine aktuelle Übersicht über alle IT-Dienstleister und Zulieferer?	☐	☐
Bewerten Sie Ihre Lieferanten systematisch nach IT-Sicherheitsrisiken?	☐	☐
Enthalten Ihre Verträge mit Dienstleistern konkrete IT-Sicherheitsanforderungen?	☐	☐
Führen Sie regelmäßig Audits oder Sicherheitsüberprüfungen bei kritischen Partnern durch?	☐	☐
Haben Sie Notfallpläne für den Ausfall eines wichtigen IT-Dienstleisters?	☐	☐
Schulen Sie Ihre Mitarbeitenden regelmäßig zum Thema IT- und Cybersicherheit und führen Sie Führen Sie interne Phishing-Tests zur Sensibilisierung durch?	☐	☐
Sind Sicherheitsrichtlinien und Verhaltensregeln allen Mitarbeitenden bekannt?	☐	☐
Haben Sie Zutrittskontrollen und physische Schutzmaßnahmen für sensible IT-Bereiche?	☐	☐
Haben Sie bereits mindestens einen vollständigen IT-Notfalltest durchgeführt (z. B. Ausfallszenario) und haben Sie im Notfall die Möglichkeit Einfuhr-, Ausfuhrpapiere zu erstellen?	☐	☐

Autorin: Julianna Straib-Lorenz

LESERFRAGEN

Muss ich meine Präferenznachweise jetzt wieder im Original vorliegen haben?

FRAGE Bei meiner letzten Zollprüfung Anfang 2024 hatten wir alle Präferenznachweise nur in Kopie vorliegen. Dies wurde so auch akzeptiert.

Nun wurde ich von der Zollstelle angeschrieben, dass sie zur Überprüfung das originale EUR.1 von uns haben wollen. Wie kann das sein?

ANTWORT VON SABINE WAZLAWIK: Laut Gesetz müssen Sie gewisse Präferenznachweise immer im Original vorliegen haben. Dies sind

- Ursprungserklärungen auf der Rechnung unter 6.000 Euro, die nicht von einem Bewilligungsinhaber ausgestellt wurden und
- förmliche Präferenznachweise wie Warenverkehrsbescheinigung EUR.1, FormA und Freiverkehrsbescheinigung A.TR.

Aufgrund der Corona-Pandemie gab es ab 1. März 2020 eine Verfügung, die besagte, dass eine Kopie des förmlichen Präferenznachweises ausreicht. Diese Verfügung wurde jedoch zum 1. April 2024 widerrufen. Das bedeutet, dass bei Ihrer letzten Zollprüfung die Ausnahmeregelung noch gegolten hat, und so Kopien anerkannt wurden. Seit 1. April 2024 ist dies jedoch nicht mehr erlaubt. Stellen Sie daher immer sicher, dass Sie im Original benötigte Präferenznachweise auch vorliegen haben. Können Sie diese auf Verlangen nicht vorzeigen, wird Ihnen die Präferenz nicht anerkannt.

Kann ich auch eine Rückware anmelden, wenn sie nicht vom damaligen Kunden zurückkommt?

FRAGE Wir erhalten immer wieder Rückwarenlieferungen unserer Maschinen, die wir dann auch innerhalb der gesetzlichen Fristen als Rückware anmelden. In vereinzelt Fällen kommen die Maschinen jedoch nicht von dem Kunden, dem wir sie damals geliefert haben,

sondern einem Dritten, da die Ware von unserem Kunden weiterverkauft wurde. Die Rückwarenbelege können wir jedoch alle vorlegen, da wir ja die Ausfuhr damals durchgeführt haben. Ist es möglich, die Ware auch in diesen Fällen als Rückwaren zollfrei anzumelden?

ANTWORT VON SABINE WAZLAWIK: Aus zollrechtlicher Sicht spricht einer Rückwarenabfertigung nichts entgegen. Das Gesetz besagt nur, dass Sie nachweisen können müssen, dass die Waren auch innerhalb der gesetzlichen Fristen wieder eingeführt wurden und es auch die entsprechenden Waren der Ausfuhr sind (Nämlichkeitssicherung). Wenn Sie dies belegen können, können Sie die Ware in den zollrechtlich freien Verkehr als Rückware anmelden und müssen keine Zollabgaben bezahlen. An-

ders ist es jedoch mit der Einfuhrumsatzsteuer. In der Regel sind Rückwaren auch von der Einfuhrumsatzsteuer befreit. Dies ist jedoch nicht der Fall, wenn die Waren im Ausland weiterverkauft wurden. Hierzu sagt das Gesetz, dass keine Befreiung der Einfuhrumsatzsteuer in Frage kommt. Daher müssen Sie bei der Zollanmeldung den EU-Code F01/03 verwenden. Vergessen Sie nicht, in Ihrem Antrag auf Rückwareneigenschaft dies auch richtig anzukreuzen, damit Sie sich Rückfragen ersparen.

GASTBEITRAG

Sabine Wazlawik

ist Dipl.-Finanzwirtin mit mehr als 10 Jahren Erfahrung im Zollbereich. Durch die tägliche Nähe zu sämtlichen Herausforderungen und Fragestellungen des Zollrechts und Außenhandels ist sie Expertin auf diesem Gebiet und unterstützt Sie als Leserin oder Leser mit ihren praktischen Tipps.

Verhindern Sie Bußgeldverfahren – Prüfen Sie Ihre Steuerbescheide auf Richtigkeit

Egal ob Sie die Zolldanmeldung selbst erstellen oder über eine Spedition. Sie sind in beiden Fällen in der absoluten Verantwortung und Haftung, falls Fehler passieren. Sie sind zudem laut Gesetz verpflichtet, die Angaben zu prüfen und bei Fehlern auch entsprechende Änderungsbescheide in Auftrag zu geben. Tun Sie dies nicht, drohen Ihnen Bußgeldverfahren. Ich zeige Ihnen, was Sie alles prüfen müssen und wie Sie bei Fehlern reagieren.



ÜBERPRÜFEN SIE IN IHRER ZOLLANMELDUNG FOLGENDE FELDER



Feld	Dies müssen Sie prüfen
Versender	Prüfen Sie, ob bei Ihrer Anmeldung der richtige Versender angegeben wurde. Ist dies nicht der Fall, vermerken Sie es auf Ihrem Steuerbescheid. Eine Änderung brauchen Sie dabei nicht in Auftrag zu geben, da sich finanziell nichts ändert. Weisen Sie jedoch den Prüfer vor der Prüfung darauf hin, dass Sie dies festgestellt haben, damit er es bei seiner Prüfung berücksichtigen kann.
Lieferbedingung	Die Zollwertberechnung steht und fällt mit der Lieferbedingung. Ist dazu etwas Falsches eingetragen, ist die Wahrscheinlichkeit hoch, dass der Zollwert falsch berechnet wurde. Ist dies der Fall, prüfen Sie den Zollwert und geben Sie Änderungen – wie am Ende des Artikels beschrieben – weiter.
Rechnungspreis	In der Praxis besteht die Gefahr, dass die der Verzollung beiliegende Rechnung nicht mit der Verzollungsrechnung übereinstimmt. Gehen Sie daher in die Buchhaltung oder in die Bestellung, um die Werte abzugleichen. Denken Sie auch daran, dass der Rechnungspreis in der Währung angegeben sein muss, die auf der Rechnung auch geschuldet wird.
Hinzurechnungen/ Abzüge	Bei der Zollwertberechnung müssen je nach Lieferbedingung noch zusätzliche Kosten wie Frachtkosten, Versicherungskosten, Verpackungskosten etc. hinzugerechnet oder abgezogen werden. Je nachdem, was im Rechnungspreis bereits enthalten ist. Gerade bei den Frachtkosten gibt es in der Praxis viele Probleme, da die Werte mit der endgültigen Frachtkostenrechnung nicht übereinstimmen.  ACHTUNG! Haben Sie oder Ihre Spedition einen Frachtkostenabzug angegeben, müssen Sie auch für diesen einen entsprechenden Nachweis haben.
Begünstigung	Haben Sie eine andere Begünstigung als 100 (normale Überführung in den zollrechtlich freien Verkehr ohne Begünstigung) angemeldet, dann müssen Sie dafür auch die jeweiligen Voraussetzungen erfüllen. 200/300/400: Ihnen müssen die entsprechenden Präferenznachweise vorliegen (bei Ursprungserklärungen unter 6.000 Euro auf der Rechnung und förmlichen Präferenznachweisen sogar im Original) 110: Ihre Ware muss genau dem Wortlaut der Einreihung entsprechen, um eine autonome Zollausssetzung in Anspruch nehmen zu können. 120: Das Kontingent muss für Ihr Lieferland und Ihre Ware gültig sein und noch Mengen frei haben.

	 ACHTUNG! Sie sehen in der Zollanmeldung, ob Ihre beantragte Begünstigung gewährt wurde. Wurde Sie Ihnen nicht gewährt, überprüfen Sie, ob vielleicht ein Eingabefehler Ihrerseits vorliegt (z. B. fehlende Unterlagen). Ist dies der Fall, können Sie einen Erstattungsantrag stellen
EU-Code	Wollen Sie Ihre Waren einfuhrabgabenfrei aufgrund beispielsweise außertariflicher Zollbefreiungen oder anderer Zollbefreiungstatbestände erhalten, müssen Sie dazu einen EU-Code angeben und alle erforderlichen Unterlagen vorlegen können. Prüfen Sie nach, ob diese Unterlagen vollständig vorliegen. Beispiel: Bei einer Rückware müssen Sie den Ausgangsnachweis sowie die Ausgangsrechnung für die Nämlichkeitsüberprüfung und die Fristeinhaltung vorlegen können.
Warentarifnummer	 MEIN TIPP Sind Sie sich unsicher mit der Einreihung, dann lassen Sie sich eine verbindliche Zolltarifauskunft von der Zollverwaltung erteilen.

So reagieren Sie richtig bei festgestellten Fehlern

Stellen Sie bei Ihrer Überprüfung Fehler fest, berechnen Sie Ihre Zollabgaben neu. Haben Sie mindestens 5 Euro je Anmeldeposition zu wenig Zollabgaben bezahlt, dann sind Sie verpflichtet, einen Nacherhebungsantrag bei dem jeweils zuständigen Haupt-

zollamt zu stellen. Handelt es sich um eine Erstattung, dann können Sie bereits ab einem Cent einen Erstattungsantrag stellen. Ich empfehle Ihnen jedoch, auch Erstattungsanträge erst ab 5 Euro zu stellen, da Sie dann einheitlich arbeiten können und der Aufwand in der Regel ansonsten nicht im Verhältnis zur Erstattung steht.

Nutzen Sie alle Vorteile Ihres Onlinebereichs!



Mehr als 200 Arbeitshilfen,
Mustervorlagen, Checklisten



Ausgaben-Archiv,
inkl. Index und Spezialreports



Webinare und
Veranstaltungen



Profitieren Sie von unserem
Expertennetzwerk:
www.zolex.de/expert





Julianna Straib-Lorenz

KURZMELDUNGEN

Zollanmeldung – Mit unserer Arbeitshilfe prüfen Sie diese immer korrekt!

Nutzen Sie unsere Checkliste, damit Ihre Zollanmeldungen stets korrekt sind. So vermeiden Sie Nacherhebungen und Ärger.

 NUTZEN SIE DIESE JA/NEIN-CHECKLISTE ZUR SCHNELLEN PRÜFUNG IHRER ZOLLANMELDUNG: 			
Feld	Prüffrage	Ja	Nein
Versender	Ist in Ihrer Anmeldung der richtige Versender angegeben und wurde ein falscher Eintrag ggf. auf dem Steuerbescheid vermerkt?	☐	☐
Lieferbedingung	Entspricht die angegebene Lieferbedingung der tatsächlichen Vereinbarung und wurde der Zollwert entsprechend korrekt berechnet?	☐	☐
Rechnungspreis	Stimmen die Werte der bezahlten Handelsrechnung mit der Verzollungsrechnung überein und ist die Währung korrekt angegeben?	☐	☐
Hinzurechnungen/ Abzüge	Wurden zusätzliche Kosten wie z B. Fracht, Versicherung, Verpackung etc. korrekt berücksichtigt und liegen entsprechende Nachweise vor?	☐	☐
Begünstigung	Entspricht die angemeldete Begünstigung den tatsächlichen Voraussetzungen und liegen alle erforderlichen Nachweise vor?	☐	☐
EU-Code	Haben Sie den richtigen EU-Code für Zollbefreiungstatbestände angegeben und sind alle zugehörigen Unterlagen vollständig vorhanden?	☐	☐
Warentarifnummer	Haben Sie die richtige Warentarifnummer angemeldet und stimmt die Warenbeschreibung mit der tatsächlichen Ware überein?	☐	☐

Autorin: Julianna Straib-Lorenz

Neue Handelsabkommen der VAE mit Costa Rica und Mauritius in Kraft

Zum 1. April 2025 sind zwei weitere Abkommen in Kraft getreten: mit Costa Rica und Mauritius.

CEPA mit Costa Rica: Fast vollständige Zollfreiheit für Exporte

Das Abkommen mit Costa Rica sieht vor, dass 99,8 % der Exporte aus den VAE und 98 % der Exporte aus Costa Rica entweder sofort oder innerhalb eines Zeitraums von bis zu zehn Jahren zollfrei gestellt werden. Damit profitieren nahezu alle Unternehmen, die Waren zwischen beiden Ländern handeln, von erheblichen Kostenvorteilen.

CEPA mit Mauritius: Zollabbau binnen fünf Jahren

Auch das CEPA mit Mauritius bietet klare Vorteile, denn über 97 % der mauritischen Ursprungswaren werden von den VAE sofort oder schrittweise zollfrei gestellt (max. Übergangsfrist: fünf Jahre). Und 99 % der Waren mit Ursprung in den VAE werden beim Import nach Mauritius ebenfalls zollfrei behandelt.

Autorin: Julianna Straib-Lorenz