

EXPORTKONTROLLE

IN DER PRAXIS

Rechtssicher handeln im Export

KW 30 | 2026



3 Sanktionsrisiken minimieren
Wie Sie mit der neuen OFAC-Broschüre Ihre Compliance-Strukturen effektiv aufbauen und absichern

4 Mercosur: Die Lieferantenerklärung entscheidet
Verwenden Sie präzise Lieferantenerklärungen und sichern Sie damit Ihre Zollpräferenzen ab

TOP-THEMA

6 Einkaufswerkzeuge für die Zoll-Compliance?!
Lückenlose Zoll-Compliance und operative Risiken im Außenhandel beherrschen Sie damit sicher

10 NIS-2 wird zur Pflicht – sind Sie betroffen?
Wenn der Cyberangriff zum Haftungsfall für die Geschäftsführung wird

EDITORIAL



Holger Schmidbaur

berät Mandanten aller Branchen und Unternehmensgrößen, ist für Seminare buchbar und gibt auch als Autor sein Wissen weiter.

Wie Sie strategische Einkaufswerkzeuge für eine lückenlose Zoll-Compliance nutzen

Liebe Leserin, lieber Leser,

jeder von uns kennt die tägliche Zerreißprobe im Außenwirtschaftsrecht. Während der Einkauf die Einstandspreise drückt, tragen wir die Verantwortung für komplexe Gesetze wie die EU-Dual-Use-Verordnung oder CBAM. Wenn Schnittstellen versagen, drohen sofort Lieferabrisse oder Bußgelder.

Ich erlebe diese Konflikte in meiner Praxis permanent. Doch wir können diese Gegensätze auflösen. Im Top-Thema auf Seite 5 erfahren Sie, wie Sie bewährte Management-Frameworks wie SWOT, PESTLE, SCOR, SIPOC und RACI in präzise Werkzeuge für Ihr Compliance-Management verwandeln. Wir binden den Einkauf direkt ein, sichern den AEO-Status und automatisieren Kontrollen im ERP-System. So steuern Sie globale Beschaffungsströme vorausschauend und schützen Ihr Unternehmen verlässlich.

Nutzen Sie diese Strategien, um Ihre Lieferkette effektiv zu stabilisieren und rechtssicher in die Zukunft zu führen.

Herzlichst Ihr

Holger Schmidbaur,
Chefredakteur

INHALTSVERZEICHNIS

NEWS 3

- ☐ Die US-Sanktionsregeln werden immer komplexer: Mit dieser Broschüre behalten Sie leicht den Überblick

NEWS 4

- ☐ Mercosur-Handel: Wie ein einziges Wort Ihren Zollsatz hochschnellen lassen kann

TOP-THEMA 5

- ☐ Zeit sparen und Risiken vermeiden: Wie Sie 5 bewährte Werkzeuge in Ihrer Außenhandels-Praxis unterstützen können

ARBEITSHILFE 8

- ☐ Strategische Symbiose: Wie Sie den Einkauf als Hebel für eine lückenlose Zoll-Compliance nutzen

LESERFRAGEN 9

- ☐ Wir haben das Thema Zoll komplett an unsere Spedition ausgeliefert. Sind wir damit auf der sicheren Seite?

GASTBEITRAG 10

- ☐ NIS-2: Wie der Cyberangriff zum Haftungsfall werden kann – bei nahezu jedem Unternehmen

KURZMELDUNGEN 12

- ☐ Zollbewilligungen ab Juni 2026: Welche Daten Sie jetzt liefern müssen

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



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

NEWS

Die US-Sanktionsregeln werden immer komplexer: Mit dieser Broschüre behalten Sie leicht den Überblick

Stellen Sie sich vor, Sie haben 2018 ein technisches Bauteil nach Ghana geliefert und plötzlich meldet sich eine US-Behörde mit einer Nachfrage zu diesem Vorgang – also fast 10 Jahre später! Das kann durchaus passieren. Und der Hinweis darauf, die entsprechenden Regeln nicht gekannt zu haben, schützt Sie nicht vor Strafen.

Das Office of Foreign Assets Control (OFAC) veröffentlicht eine umfassende Einführung, die Unternehmen als zentraler Wegweiser dient. Diese Publikation verdeutlicht, dass US-Sanktionen nicht an nationalen Grenzen enden. Sobald US-Ursprungswaren, Technologien oder Finanztransaktionen in US-Dollar den Geschäftsprozess berühren, greift die US-Rechtsordnung. Sie müssen diese globale Reichweite in Ihre tägliche Risikobewertung einbeziehen, da die Behörde selbst bei fehlender Kenntnis der Sanktionsverstöße eine strikte zivilrechtliche Haftung anwendet.

Was die OFAC konkret von deutschen Firmen erwartet

OFAC erwartet von Unternehmen ein maßgeschneidertes, risikobasiertes Compliance-Programm, das weit über die reine Sanktionslistenprüfung hinausgeht. Zentral ist eine umfassende Risikoanalyse, die Produkte, Geschäftspartner, Lieferketten, Zahlungsströme und Zielmärkte systematisch bewertet und dabei sowohl direkte als auch indirekte Sanktionsrisiken berücksichtigt.

Auf dieser Grundlage sollten Sie die 5 Kernelemente eines wirkamen OFAC-Programms konsequent verankern: Management-Engagement, eine belastbare Risikobewertung, klar definierte interne Kontrollen, regelmäßige Tests und Audits sowie zielgruppenspezifische Schulungen für alle relevanten Funktionen. Ergänzend empfiehlt OFAC den Einsatz technischer Präventionsmaßnahmen, etwa automatisierter Geolokalisierungs- und IP-Filter, um Zugriffe aus sanktionierten Regionen frühzeitig zu blockieren und Umgehungsversuche zu verhindern. Ebenso sinnvoll sind Monitoring-Mechanismen, die ungewöhnliche Transaktionsmuster oder Auffälligkeiten bei Neukunden automatisch markieren. So entsteht ein integriertes Compliance-System, das Risiken nicht nur erkennt, sondern aktiv steuert und dokumentiert – ein entscheidender Faktor für die Rechtssicherheit und die Glaubwürdigkeit Ihres Unternehmens gegenüber Behörden.

Was die 10-jährige Verjährungsfrist für Ihre Praxis bedeutet

Weil viele Sanktionsverstöße inzwischen erst nach 10 Jahren verjähren, müssen Unternehmen ihre Prüfungen und Entscheidungen länger dokumentieren. Speichern Sie sämtliche Nachweise zu Prüfungen und Transaktionen für diesen Zeitraum sicher ab. Bereiten Sie im Falle einer Unregelmäßigkeit zudem das Szenario

einer freiwilligen Selbstanzeige vor, da dieses Vorgehen laut Enforcement Guidelines potenzielle Geldbußen erheblich reduziert.

Verantwortlichkeiten im Unternehmen verteilen und abteilungsübergreifend zusammenarbeiten

Um die Compliance-Anforderungen umzusetzen, binden Sie folgende Abteilungen aktiv ein:

-  **Vertrieb:** Erstellen Sie verbindliche Vorgaben für die Prüfung neuer Geschäftspartner, bevor Verträge entstehen. Die Vertriebsmitarbeiter tragen die Verantwortung für die erste Einschätzung des Kundenrisikos.
-  **IT-Abteilung:** Implementieren Sie automatisierte Screening-Software, die regelmäßig aktualisierte Sanktionslisten prüft. Richten Sie zudem IP-basierte Geolokalisierungssperren für kritische Webportale ein.
-  **Logistik:** Kontrollieren Sie den Ursprung der Waren und die Transitwege lückenlos. Dokumentieren Sie jeden US-Bezug in der Lieferkette, um den Reexport-Status jederzeit nachzuweisen.
-  **Geschäftsführung:** Verankern Sie das Commitment zur Compliance als festen Bestandteil der Unternehmenskultur. Stellen Sie die notwendigen Ressourcen für Schulungen und Audits bereit.



FAZIT

Die neue OFAC-Broschüre (<https://bit.ly/3TdaWyr>) unterstreicht eindrücklich, wie unverzichtbar proaktive Compliance-Maßnahmen in einem zunehmend komplexen globalen Marktumfeld geworden sind. Sie zeigt nicht nur typische Risikofelder auf, sondern liefert zugleich konkrete Hinweise, wie Unternehmen ihre internen Kontrollmechanismen stärken und Schwachstellen systematisch identifizieren können. Nutzen Sie diesen Leitfaden als fundierte Grundlage, um bestehende Prozesse kritisch zu überprüfen, Verantwortlichkeiten klar zuzuordnen und technische wie organisatorische Schutzmaßnahmen zu verbessern.

Autor: Holger Schmidbaur

Mercosur-Handel: Wie ein einziges Wort Ihren Zollsatz hochschnellen lassen kann

Stellen Sie sich vor, Ihre Sendung in einen Mercosur-Staat bleibt am Zoll hängen, weil Sie auf der Lieferantenerklärung für Waren mit Präferenzursprungseigenschaft lediglich einzelne Länder statt des geforderten Begriffs „MERCOSUR“ angeben. Solche vermeintlich kleinen Fehler führen oft zu kostspieligen Verzögerungen und belasten Ihre Zoll-Compliance massiv. So umgehen Sie Stolperfallen.

Achten Sie auf die korrekte Kennzeichnung

Die deutsche Zollverwaltung stellt klar, dass bei der Ausfertigung von Lieferantenerklärungen für die betroffenen Staaten ausschließlich die offizielle Abkürzung „MERCOSUR“ zählt. Die bloße Nennung einzelner Mitgliedsstaaten reicht in diesem Kontext nicht aus. Auch wenn Sie einzelne Staaten ergänzend in Klammern aufführen dürfen, bleibt die Verwendung des übergeordneten Begriffs zwingend vorgeschrieben. Dies dient der einheitlichen Dokumentation und vermeidet Interpretationsspielräume bei der Zollprüfung.

Was hinter den Kennzeichnungsregeln steckt – und worauf Sie achten sollten

Der Hintergrund dieser strikten Anforderung liegt in der zwingenden Notwendigkeit einer eindeutigen und rechtssicheren Kennzeichnung in allen Warenursprungsunterlagen. Präzise und konsistente Bezeichnungen sind ein zentrales Element der Präferenzdokumentation, da sie den Behörden ermöglichen, die Herkunft der Ware zweifelsfrei nachzuvollziehen.

Verwenden Unternehmen hingegen abweichende oder uneinheitliche Begriffe, riskieren sie die Nichtanerkennung der Präferenz, was unmittelbar zu höheren Zollsätzen führt. Dies wirkt sich direkt auf die Kostenstruktur und Wettbewerbsfähigkeit Ihrer Kunden aus und kann die Attraktivität Ihrer Produkte im Zielmarkt erheblich mindern.

Darüber hinaus schützt eine saubere, nachvollziehbare Dokumentation Ihr Unternehmen im Rahmen von Betriebs- und Nachprüfungen. Klare Ursprungsangaben reduzieren das Risiko nachträglicher Korrekturen, Rückforderungen oder gar Bußgelder. Eine konsistente Terminologie ist damit nicht nur formale Pflicht, sondern ein wesentlicher Bestandteil eines belastbaren, revisionssicheren Ursprungs- und Präferenzsystems.

Organisieren Sie Ihre Prozesse neu und koordinieren Sie Ihre Abteilungen für fehlerfreie Lieferantendokumente

Damit Sie diese Vorgaben sicher umsetzen, bedarf es einer klaren Abstimmung innerhalb Ihres Unternehmens:

- 🌐 **Exportkontrolle und Zoll:** Überprüfen Sie Ihre aktuellen Vorlagen für Lieferantenerklärungen. Ersetzen Sie länderspezifische Angaben sofort durch den festen Begriff „MERCOSUR“.
- 🌐 **Vertrieb:** Informieren Sie Ihr Vertriebsteam über die neuen Anforderungen, damit dieses Kundenanfragen kompetent beantwortet und keine veralteten Dokumente verspricht.
- 🌐 **IT:** Passen Sie Ihre ERP-Systeme sowie die Stammdatenpflege an. Stellen Sie sicher, dass bei der Generierung von Lieferantenerklärungen für diesen Wirtschaftsraum automatisiert der korrekte Begriff „MERCOSUR“ hinterlegt ist.
- 🌐 **Logistik:** Schulen Sie Ihre Mitarbeiter bei der Eingangsprüfung von Lieferantenerklärungen. Reklamieren Sie Dokumente, die diesen Standard nicht erfüllen, konsequent bei Ihren Lieferanten.



FAZIT

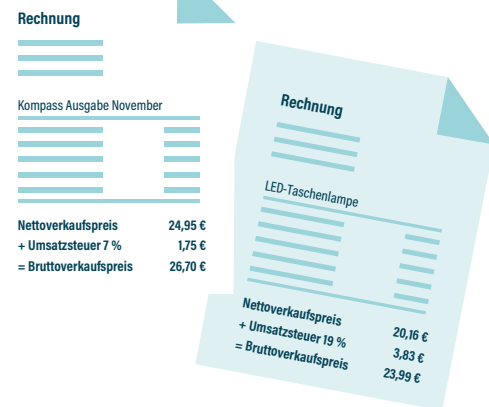
Die korrekte Bezeichnung „MERCOSUR“ in Lieferantenerklärungen verhindert Verzögerungen bei der Zollabfertigung und sichert Ihre Präferenzvorteile zuverlässig ab. Prüfen Sie Ihre Unterlagen, passen Sie Ihre IT-Systeme an und schulen Sie die relevanten Abteilungen, damit alle Prozesse durchgängig rechtskonform ablaufen. So stellen Sie sicher, dass Ihr Unternehmen in diesem wichtigen Handelsraum jederzeit präferenzfähig bleibt und Risiken aus fehlerhaften Ursprungsangaben frühzeitig ausgeschlossen werden.

Autor: Holger Schmidbaur

TOP-THEMA

Zeit sparen und Risiken vermeiden: Wie 5 bewährte Werkzeuge Sie in Ihrer Außenhandels-Praxis unterstützen können

Der Einkauf schaut nur auf den Einstandspreis – und die Außenhandelsabteilung darf sich um die Compliance kümmern. Das ist in vielen Betrieben leider an der Tagesordnung. Dadurch steigt die Arbeitsbelastung für die Verantwortlichen weiter. Doch mit 5 erprobten Management-Werkzeugen lässt sie sich senken. So finden Sie Ihren persönlichen „Zeitsparer“.



Die Realität im globalen Handel zeigt, dass eine mangelhafte Abstimmung zwischen dem strategischen Einkauf und der Zollabteilung existenzbedrohliche Folgen nach sich zieht. Wenn Einkäufer Verträge mit internationalen Lieferanten abschließen, ohne die exportkontrollrechtlichen Implikationen zu prüfen, drohen erhebliche Verzögerungen, Bußgelder oder der vollständige Verlust von Einfuhrgenehmigungen. Das Außenwirtschaftsrecht und die Compliance dürfen daher niemals als nachgelagerte Kontrollinstanz agieren, sondern müssen direkt in den Beschaffungsprozess einfließen.

Das Spannungsfeld zwischen Kostenoptimierung und Rechtssicherheit

Der Einkauf fokussiert sich traditionell auf die Reduzierung von Einstandspreisen, die Absicherung von Lieferkapazitäten und die Optimierung von Zahlungszielen.

Demgegenüber steht die Pflicht der Zoll- und Exportkontrollbeauftragten, die Einhaltung komplexer rechtlicher Rahmenbedingungen wie der EU-Dual-Use-Verordnung (Verordnung (EU) 2021/821) oder EU- nationaler Embargobestimmungen zu garantieren. Ein klassisches Konfliktszenario entsteht, wenn ein Einkäufer eine neue, kostengünstige Komponente für eine Industrieanlage in einem Drittland bestellt, die aufgrund ihrer technischen Spezifikationen einer Ausfuhr- oder Verwendungsbeschränkung unterliegt. Wird diese Prüfung versäumt, greifen bei der Einfuhr oder dem späteren Re-Export strenge Sanktionen. Die Integration strategischer Frameworks ermöglicht es Ihnen, diesen Gegensatz aufzulösen und Compliance als integralen Bestandteil der Lieferantenqualifizierung zu etablieren.

Wie Sie die 5 zentralen Methodiken für Ihre Zoll- und Exportkontrollprozesse adaptieren

Die im strategischen Management etablierten Werkzeuge SWOT, PESTLE, SCOR, SIPOC und RACI bieten eine hervorragende Struktur, um die Brücke zwischen der Beschaffungswelt und den zollrechtlichen Anforderungen zu schlagen. Sie helfen Ihnen dabei, Risiken systematisch zu identifizieren, Prozesse transparent abzubilden und Verantwortlichkeiten unmissverständlich zuzuweisen.

Die SWOT-Analyse: Interne Stärken nutzen und externe Bedrohungen im Zollrecht proaktiv abwenden

Die SWOT-Analyse dient Ihnen dazu, die interne Leistungsfähigkeit Ihrer Zoll- und Exportkontrollorganisation im Verhältnis zu den dynamischen Veränderungen des globalen Handelsumfelds zu bewerten.

- 🌐 **Strengths (Stärken):** Hierzu zählen ein hoher Automatisierungsgrad in Ihrem ERP-System, zertifizierte Mitarbeiter oder der Status als zugelassener Wirtschaftsbeteiligter (AEO-C und AEO-S). Diese Stärken ermöglichen Ihnen eine beschleunigte Zollabwicklung.
- 🌐 **Weaknesses (Schwächen):** Typische Schwachstellen betreffen unzureichende Ressourcen für die Tarifierung, lückenhafte Stammdaten oder eine mangelhafte Kommunikation zwischen Einkauf und Zoll.
- 🌐 **Opportunities (Chancen):** Die Nutzung von Freihandelsabkommen oder die Implementierung digitaler Tools zur Sanktionslistenprüfung bieten enorme Potenziale zur Kostensenkung und Risikominimierung.

- Threats (Risiken): Verschärfungen von Embargos, kurzfristige Änderungen von Zollsätzen (z. B. durch Handelskonflikte) oder strengere Auslegungsvorschriften der Zollbehörden gefährden die Stabilität Ihrer Lieferkette.

Die PESTLE-Analyse: Globale Makro-Risiken für die Exportkontrolle systematisch scannen

Mit der PESTLE-Analyse betrachten Sie die externen Einflussfaktoren, die sich unmittelbar auf Ihre zollrechtliche Compliance und Ihre Beschaffungsweg auswirken:

- Political (Politisch): Geopolitische Spannungen führen zu veränderten Sanktionslisten. Sie müssen kontinuierlich überwachen, welche Länder oder Personen neuen Restriktionen unterliegen.
- Economic (Ökonomisch): Wechselkursschwankungen und Strafzölle verändern den Zollwert von Waren, was direkte Auswirkungen auf die zu entrichtenden Einfuhrabgaben hat.
- Social (Sozial): Das gesellschaftliche Bewusstsein für Menschenrechte zwingt Gesetzgeber zu Initiativen wie dem Lieferkettensorgfaltspflichtengesetz (LkSG). Sie müssen nachweisen, dass Ihre Lieferanten Sozialstandards einhalten.
- Technological (Technologisch): Die Digitalisierung der Zollbehörden (z. B. ATLAS in Deutschland oder neue EU-weite Zollsyste) erfordert eine ständige Anpassung Ihrer IT-Schnittstellen.
- Legal (Rechtlich): Die kontinuierliche Weiterentwicklung der EU-Dual-Use-Verordnung verlangt eine präzise technische Überwachung Ihrer Produkte, um Genehmigungspflichten rechtzeitig zu erkennen.
- Environmental (Umweltbezogen): Neue Instrumente wie das CO₂-Grenzausgleichssystem (CBAM) der EU erlegen Importeuren umfangreiche Berichtspflichten und zusätzliche finanzielle Belastungen auf.

Das SCOR-Modell: Die zollrechtliche Kette vom Vorlieferanten bis zum Endkunden lückenlos verknüpfen

Das Supply Chain Operations Reference (SCOR)-Modell gliedert Ihre Prozesse in die Bereiche Planen, Beschaffen, Herstellen, Liefern und Zurücksenden. Aus Sicht der Außenwirtschaft müssen Sie in jede dieser Phasen Kontrollpunkte integrieren:

Planen (Plan): Definieren Sie bereits in der Planungsphase klare Exportkontroll- und Zollprozesse.

- Beschaffen (Source): Bei der Lieferantenauswahl fordern Sie zwingend verbindliche Lieferantenerklärungen und die Angabe der statistischen Warennummern an.
- Herstellen (Make): Während der Produktion müssen Sie den zollrechtlichen Ursprung überwachen. Verarbeiten Sie Vormaterialien ohne Ursprungsbezeichnung, verändert dies potenziell den Präferenzstatus des Endprodukts gemäß den jeweiligen Ursprungsregeln.

- Liefern (Deliver): Vor dem physischen Versand der Ware erfolgt die finale Sanktionslistenprüfung des Empfängers sowie die Prüfung, ob eine Ausfuhrgenehmigungspflicht nach der Dual-Use-Verordnung vorliegt.
- Zurücksenden (Return): Bei Warenrücksendungen prüfen Sie, welche zoll- und exportkontrollrechtlichen Anforderungen für die Wiedereinfuhr oder den erneuten Versand gelten. Dokumentieren Sie den Rücksendeprozess vollständig und stellen Sie sicher, dass Genehmigungs- und Nachweispflichten auch im Retourenfall eingehalten werden.

Das SIPOC-Diagramm: Prozesse visualisieren und Schnittstellenrisiken eliminieren

Das SIPOC-Framework (Suppliers, Inputs, Process, Outputs, Customers) erlaubt es Ihnen, einen zollrelevanten Teilprozess auf einer einzigen Seite transparent darzustellen. Dadurch erkennen Sie sofort, an welchen Stellen unvollständige Informationen in das System einfließen. Wenn etwa der Lieferant eine Handelsrechnung ohne präzise Warenbeschreibung liefert, kann die Zollabteilung bei der „Zollanmeldung“ keine korrekte Tarifierung vornehmen, was zu Verzögerungen beim Zollamt führt.

Die RACI-Matrix: Eindeutige Verantwortlichkeiten für die Compliance festlegen

Verantwortlichkeiten im Außenwirtschaftsrecht dürfen keine Grauzonen haben. Die RACI-Matrix weist Rollen eindeutig zu: Responsible für die operative Durchführung, Accountable für die rechtliche Gesamtverantwortung, Consulted für Beratung und Informed für reine Information. Der Ausfuhrverantwortliche – meist Vorstand oder Geschäftsführung – bleibt stets Accountable für die Exportkontrolle, während der Zollbeauftragte die operativen Aufgaben als Responsible übernimmt.

Wie Sie die Frameworks in der betrieblichen Praxis verankern

Die nachfolgende Übersicht verdeutlicht, wie Sie die 5 Management-Werkzeuge konkret für die Belange Ihrer Zoll- und Exportkontrollorganisation konfigurieren.

Konkrete Praxisbeispiele

Um die praktische Wirksamkeit dieser Frameworks zu demonstrieren, betrachten wir 2 detaillierte Szenarien aus der industriellen Praxis.

Fallbeispiel 1: Beschaffung von Industriekomponenten mit potenziellem Dual-Use-Charakter

Ein mittelständischer Maschinenbauer plant den Einkauf hochpräziser Ventile für eine neue Anlage. Der strategische Einkauf findet einen günstigen Lieferanten in Südkorea. Aufgrund von Material und Druckbeständigkeit könnten die Ventile jedoch unter Position 2B350 des Anhangs I der EU-Dual-Use-Verordnung fallen.

Schritt 1: Anwendung des SIPOC-Frameworks zur Prozesstransparenz

Um den Prozess der Beschaffung sauber aufzusetzen, erstellt der Zollbeauftragte gemeinsam mit dem Einkauf folgendes SIPOC-Modell:

- 🌐 **Supplier:** Südkoreanischer Ventilhersteller
- 🌐 **Input:** Technisches Datenblatt, CAD-Zeichnungen, Materialzertifikate, Angebot mit Lieferbedingungen (Incoterms 2020: FCA)
- 🌐 **Process:** 1. Bereitstellung der technischen Unterlagen durch den Einkauf an die Zollabteilung
 1. Abgleich der Parameter mit der Ausfuhrliste und der Dual-Use-Güterliste durch den Exportkontrollbeauftragten
 2. Feststellung der Genehmigungspflicht für den eventuellen Re-Export oder die Verwendung
 3. Hinterlegung der Codierung im ERP-System
- 🌐 **Output:** Klassifizierte Materialstammdaten (HS-Code, Dual-Use-Kennzeichen), gegebenenfalls vorliegende Endverbleibserklärung (End-User Certificate)
- 🌐 **Customer:** Operativer Einkauf (für die Bestellung), Logistik (für die Zollanmeldung), Zollbehörde

Schritt 2: Verteilung der Aufgaben über die RACI-Matrix

Um sicherzustellen, dass keine Prüfschritte übersprungen werden, greift die folgende RACI-Zuordnung:

- 🌐 **Einholen der technischen Datenblätter beim Lieferanten:** Einkauf (Responsible), Zollbeauftragter (Consulted), Logistikleiter (Informed). Die Gesamtverantwortung (Accountable) für den Prozessschritt verbleibt beim Einkaufsleiter.
- 🌐 **Technische Einstufung (Güterklassifizierung):** Exportkontrollbeauftragter (Responsible), Technischer Vertrieb/Konstruktion (Consulted). Der Ausführungsverantwortliche des Vorstands ist hier (Accountable).
- 🌐 **Beantragung der Ausfuhrgenehmigung beim BAFA (falls erforderlich):** Zollbeauftragter (Responsible), Ausführungsverantwortlicher (Accountable), Einkauf (Informed)

Fallbeispiel 2: Implementierung des CO₂-Grenzausgleichssystems (CBAM) beim Import von Aluminium- und Stahlprodukten

Ein Automobilzulieferer in Deutschland importiert große Mengen spezifischer Aluminiumstrangpressprofile aus der Türkei und China. Seit Einführung des CBAM nach Verordnung (EU) 2023/956 muss das Unternehmen die Emissionen erfassen, quartalsweise melden und entsprechende CBAM-Zertifikate erwerben.

Schritt 1: Anwendung der PESTLE-Analyse zur Risikoidentifikation

Die Zollabteilung nutzt die PESTLE-Analyse, um die Tragweite dieser neuen gesetzlichen Anforderung für das Unternehmen transparent zu machen:

- 🌐 **Political:** Die EU verfolgt das Ziel der Klimaneutralität („Fit for 55“). CBAM dient dazu, die Verlagerung von CO₂-Emissionen in Drittländer ohne strenge Klimauflagen (Carbon Leakage) zu verhindern.
- 🌐 **Economic:** Die Notwendigkeit, CBAM-Zertifikate abzukauften, erhöht die Einstandskosten für Aluminium aus Ländern mit hohem CO₂-Ausstoß drastisch. Dies beeinflusst die Marge der Endprodukte negativ.
- 🌐 **Technological:** Der Importeur muss IT-Systeme etablieren, die in der Lage sind, verifizierte Emissionsdaten der Lieferanten direkt im Beschaffungsprozess zu verarbeiten und an das zentrale CBAM-Register der EU zu übermitteln.
- 🌐 **Legal:** Versäumt das Unternehmen die Abgabe der vierteljährlichen CBAM-Berichte oder zertifiziert es sich nicht rechtzeitig als „zugelassener CBAM-Anmelder“, drohen empfindliche Bußgelder von bis zu 50 € pro Tonne nicht gemeldeter Emissionen.

Schritt 2: Anwendung des SCOR-Modells zur operativen Umsetzung

Das Unternehmen strukturiert die Implementierung entlang des SCOR-Modells, um die Berichtspflichten tief in der Lieferkette zu verankern:

- 🌐 **Planen (Plan):** Die Zollabteilung analysiert anhand der Zoll-Tarifnummern (Kapitel 76 für Aluminium), welche importierten Artikel unter die CBAM-Verordnung fallen. Der Einkauf schätzt die zukünftigen Importvolumina ab.
- 🌐 **Beschaffen (Source):** Bei Verhandlungen mit den Lieferanten in der Türkei und China wird die Bereitstellung valider Emissionsdaten (berechnet nach den EU-Vorgaben) als vertragliche Hauptpflicht verankert. Liefert ein Lieferant keine Daten, löst dies einen automatischen Lieferantenwechsel aus.
- 🌐 **Liefern (Deliver):** Bei der Einfuhrabwicklung stellt der Zollspediteur sicher, dass die Zollanmeldung die notwendigen CBAM-relevanten Daten enthält und die Verknüpfung mit der EORI-Nummer des zugelassenen CBAM-Anmelders fehlerfrei erfolgt.

Dieses Vorgehen bewahrt das Unternehmen vor unerwarteten Nachzahlungen und sichert den kontinuierlichen Zufluss kritischer Produktionsmaterialien.

FAZIT

Frameworks wie SWOT, PESTLE, SCOR, SIPOC und RACI bilden die Basis eines proaktiven ICP. Konsequente Anwendung schafft transparente Abläufe, klare Verantwortlichkeiten und schützt zuverlässig vor Reputationsschäden, Bußgeldern und Lieferabbrüchen.

Autor: Holger Schmidbaur



Strategische Symbiose: Wie Sie den Einkauf als Hebel für eine lückenlose Zoll-Compliance nutzen

Die folgende Übersicht zeigt Ihnen präzise, wie Sie die strategischen Methoden schrittweise in die Praxis umsetzen, Schnittstellen zu anderen Abteilungen definieren und die notwendigen internen Compliance-Strukturen etablieren.

 ÜBERSICHT: SICHERN SIE BEIM EINKAUF DIE LÜCKENLOSE ZOLL-COMPLIANCE 				
Schritt	Frame- work	Operative Umsetzung & Maß- nahmen	Einzubindende Abteilungen	Zu erstellende Arbeits- und Organisationsan- weisungen (AWB)
1. Strategische Risikoanalyse	SWOT & PESTLE	Sie scannen geopolitische und makroökonomische Veränderungen (z. B. CBAM, Embargos). Parallel bewerten Sie interne Stärken (AEO-Status) und Schwächen (Stammdatenqualität).	Strategischer Einkauf Zoll/Exportkontrolle Geschäftsleitung	AWB Frühwarnsystem Außenhandel: Regelung des Turnus zur Überwachung von Gesetzesänderungen und Sanktionslisten
2. Prozess- und Schnittstellen-Mapping	SIPOC	Sie visualisieren den Informations- und Datenfluss vom Lieferanten bis zur Zollanmeldung. Dadurch eliminieren Sie Schnittstellenrisiken, wie unvollständige Handelsrechnungen.	Operativer Einkauf Logistik/Wareneingang IT/Stammdatenpflege	AWB Stammdatenerfassung Import: Vorgabe von Pflichtfeldern (HS-Code, Ursprungsland) bei der Neuanlage von Artikeln
3. Pflichtenheft für die Lieferkette	SCOR (Source & Make)	Bei Verhandlungen verankern Sie die Pflicht zur Bereitstellung von Langzeit-Lieferantenerklärungen, technischen Datenblättern und CBAM-Emissionswerten direkt im Vertrag.	Strategischer Einkauf Qualitätsvorplanung Rechtsabteilung	AWB Lieferanten-Compliance: Richtlinie zur zollrechtlichen Bewertung von Lieferanten und Nutzung sicherer Incoterms (z. B. FCA/DAP)
4. Technische Güterprüfung	SIPOC & RACI	Nach Erhalt der technischen Daten führen Sie eine präzise Klassifizierung durch. Sie prüfen das Material auf Dual-Use-Eigenschaften (z. B. Anhang I EU-Dual-Use-VO) und hinterlegen Genehmigungspflichten im ERP.	Exportkontrolle Technische Konstruktion F&E/Produktion	AWB Güterklassifizierung und Exportkontrolle: Verfahren zur technischen Prüfung und zum Umgang mit BAFA-Genehmigungen
5. Operative Freigabe & System-Check	RACI	Sie implementieren automatisierte „Quality Gates“ im ERP-System. Jede Bestellung oder Ausfuhr wird erst nach erfolgreicher Sanktionslistenprüfung und Zoll-Tarifierung freigegeben.	IT/Systemadministration Zollabteilung Versand/Logistik	AWB Systemgestützte Compliance-Prüfung: Prozessbeschreibung bei System-Sperren („Matches“) und Verteilung der Freigabebefugnisse

Autor: Holger Schmidbaur

LESERFRAGEN

Wir haben das Thema Zoll komplett an unsere Spedition ausgeliefert. Sind wir damit auf der sicheren Seite?

FRAGE Wir geben unsere Exportprozesse komplett aus der Hand: Eine spezialisierte Spedition übernimmt bei uns den Versand inklusive der gesamten Zollabwicklung. Dennoch erhalten wir regelmäßige Rückfragen vom Zollamt oder festgestellte Fehler bei der

Ausfuhranmeldung. Wie ist unsere Haftung als Exporteur tatsächlich zu bewerten, wenn wir den physischen Prozess und die Anmeldung vollständig an Dritte übertragen haben? Verfällt unsere Verantwortung als Ausführer mit der Beauftragung des Dienstleisters?

ANTWORT **VON HOLGER SCHMIDBAUR:** Viele exportierende Unternehmen glauben fälschlich, dass die Beauftragung eines Logistikdienstleisters oder Zollagenten die eigene Verantwortung für Exportkontrolle und Zollrecht überträgt. Nach dem Zollrecht der EU (Unionszollkodex, UZK) bleibt jedoch der Ausführer verantwortlich, da er die Ware aus dem Zollgebiet verbringt bzw. verbringen lässt und zum Zeitpunkt der Anmeldung über sie verfügt. Die Einschaltung eines Dritten – ob direkte oder indirekte Vertretung – ändert nichts an dieser primären Sorgfaltspflicht. Fehler wie falsche Zolltarifnummern, unvollständige Werte oder übersehene Sanktionslisten des Dienstleisters fallen unmittelbar auf den Exporteur zurück.

Auswirkungen auf die tägliche Arbeit: Diese Fehlannahme führt in Unternehmen häufig zu mangelnder Kontrolle der durch den Dienstleister eingereichten Dokumente. Wenn keine regelmäßige Prüfung der erstellten Ausfuhrbegleitdokumente (ABD) erfolgt, entstehen bei Betriebsprüfungen durch die Zollverwaltung erhebliche Risiken, die von Bußgeldern bis hin zum Entzug des Status als „Zugelassener Wirtschaftsbeteiligter“ (AEO) reichen können. Die tägliche Praxis zeigt, dass die operative Bequemlichkeit die rechtliche Absicherung gefährdet.

Handlungsempfehlungen

Implementierung eines Kontrollsystems: Sie etablieren einen Prozess zur nachträglichen Prüfung aller durch den Dienstleister eingereichten Zollanmeldungen anhand der vorliegenden Handelsrechnungen und Packlisten.

Schriftliche Fixierung der Weisungen: Sie treffen klare vertragliche Vereinbarungen mit dem Dienstleister, in denen die Art der Vertretung und die Informationspflichten bei Abweichungen exakt definiert sind.

Regelmäßige Audits: Sie führen in festen Intervallen Stichprobenprüfungen der vom Dienstleister übermittelten Datensätze durch, um die Qualität der Arbeit zu überwachen.

Nutzung eigener EORI-Nummern: Sie stellen sicher, dass Ihre EORI-Nummer stets korrekt verwendet wird und Sie Zugriff auf das Portal zur Überwachung der Ausfuhrvorgänge haben.

Interne Kooperation

Um die Einhaltung der Zollvorgaben sicherzustellen, binden Sie folgende Abteilungen aktiv ein:

Logistik: Sie verantwortet die Bereitstellung korrekter Packdaten und Frachtdokumente, die als Grundlage für die Zollanmeldung dienen.

Vertrieb: Er sorgt für die vollständige Dokumentation und korrekte Anwendung der Incoterms® und stellt sicher, dass die vertraglich vereinbarten Exportbedingungen mit den Zollvorgaben korrespondieren.

IT: Sie konfiguriert Schnittstellen so, dass exportrelevante Daten (Stammdaten, Klassifizierungen) konsistent an den Dienstleister übermittelt werden, um Medienbrüche und manuelle Fehler zu vermeiden.

Fazit

Die Delegation der operativen Zollabwicklung entbindet den Exporteur nicht von seiner rechtlichen Verantwortung. Der Dienstleister bleibt reiner Erfüllungsgehilfe, während der Exporteur die Letztverantwortung für korrekte Deklarationen trägt. Für Sie und Ihr Unternehmen bedeutet das, dass ein belastbares internes Kontrollsystem unerlässlich ist, um das Haftungsrisiko wirksam zu begrenzen. Sorgen Sie für engmaschige interne Kontrollen.

GASTBEITRAG**Julianna Straib-Lorenz**

ist Unternehmensberaterin mit mehr als 16 Jahren Erfahrung im operativen Zoll- und Logistikbereich sowie in der Beratung und Schulung von Firmen. Durch ihre Tätigkeit als Dozentin bei der IHK kann sie Ihnen auch komplexe Themen verständlich erklären.

NIS-2: Wie der Cyberangriff zum Haftungsfall werden kann – bei nahezu jedem Unternehmen

Ein einziger Cyberangriff auf Ihren IT-Dienstleister – und plötzlich haftet Ihre Geschäftsführung persönlich. Klingt wie im Film, ist aber Realität geworden. Mit der NIS-2-Richtlinie (Richtlinie (EU) 2022/2555) wird Cybersicherheit für den Außenhandel zur Pflicht: direkt für viele Import- und Exportunternehmen, indirekt über die Lieferkette für nahezu alle. Was das für Ihre Compliance bedeutet und wo die persönliche Haftung beginnt, lesen Sie hier.



ÜBERSICHT: ENTGEHEN SIE DER HAFTUNGSFALLE NIS-2



Der regulatorische Rahmen: NIS-2 kommt – auch für den Mittelstand

Die NIS-2-Richtlinie der EU und das darauf aufbauende deutsche Umsetzungsgesetz – das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – markieren eine neue Ära der Cybersicherheitsregulierung. Die Richtlinie (EU) 2022/2555 ersetzt die bisherige NIS-Richtlinie aus dem Jahr 2016 und erweitert den Anwendungsbereich erheblich: Insgesamt 18 Wirtschaftssektoren werden direkt angesprochen.

Direkte Betroffenheit: Sind Sie dabei?

Direkt in den Anwendungsbereich fallen Unternehmen, die als „besonders wichtige“ oder „wichtige Einrichtungen“ klassifiziert werden. Maßgeblich sind Größe, Branche und gesellschaftliche Relevanz. Zu den direkt regulierten Sektoren gehören Energieversorgung, Gesundheitswesen, Wasserwirtschaft, Transportsektor, Finanzwirtschaft, digitale Infrastruktur und die öffentliche Verwaltung. **Auch wenn Ihr Unternehmen formal nicht zu den 30.000 direkt betroffenen Einrichtungen zählt, können Sie trotzdem in die Pflicht genommen werden. § 28 des deutschen BSI-Gesetzentwurfs nimmt zwar „vernachlässigbare“ Tätigkeiten aus dem Anwendungsbereich aus – definiert diesen Begriff jedoch nicht. Unternehmen mit einer regulierten Nebentätigkeit (z. B. digitale Dienstleistungen neben dem klassischen Außenhandel) können in den Anwendungsbereich fallen, obwohl ihre Hauptgeschäftstätigkeit nicht reguliert ist.**

In Deutschland werden insgesamt etwa 30.000 Unternehmen als direkt betroffen eingestuft.

Prüfen Sie für Ihr Unternehmen, ob Sie:

- 🌐 digitale Dienste für Kunden bereitstellen (z. B. Online-Plattformen für Bestellabwicklung)
- 🌐 Teil einer kritischen Lieferkette sind (z. B. Zulieferer für Unternehmen der Energie- oder Gesundheitsbranche)
- 🌐 IT-Dienstleistungen für kritisch eingestufte Sektoren erbringen oder empfangen

Fällt Ihr Unternehmen in eine dieser Kategorien, droht bei Nichterfüllung der Pflichten sofortige bußgeldbewehrte Compliance – ohne Übergangsfrist.

Indirekte Betroffenheit: Der Druck aus der Lieferkette

Auch wer formal nicht zur Zielgruppe gehört, gerät unter Druck – sobald größere Geschäftspartner NIS-2-pflichtig sind. Die Richtlinie verpflichtet betroffene Unternehmen, ihre Lieferketten systematisch zu analysieren und sicherzustellen, dass externe Partner angemessene Sicherheitsstandards einhalten.

Konkret bedeutet das für Außenhandelsunternehmen: Ihre Kunden und Auftraggeber werden Sicherheitsanforderungen vertraglich weitergeben, Audits einfordern und im Zweifel den Lieferanten wechseln, der nicht nachweislich NIS-2-konform arbeitet. Besonders betroffen sind:

- 🌐 **Logistikunternehmen**, die essenzielle Dienstleistungen für regulierte Sektoren wie Energie, Gesundheit oder Lebensmittel erbringen
- 🌐 **Maschinenbauer und Komponentenhersteller**, die in globale Lieferketten eingebunden sind und für NIS-2-pflichtige Industrieunternehmen produzieren
- 🌐 **IT-Dienstleister und Cloud-Anbieter**, die die technische Basis für betroffene Organisationen stellen
- 🌐 **Handelsunternehmen**, die ERP-Systeme oder digitale Plattformen nutzen und mit kritischen Sektoren kooperieren – etwa im Großhandel für medizinische Geräte oder Chemikalien

Risikomanagement: Was das Gesetz konkret fordert

Direkt betroffene Unternehmen müssen ein umfassendes Risikomanagementsystem für ihre IT-Infrastruktur einführen. Zu den Pflichtmaßnahmen gehören:

- 🌐 Durchführung von Risikoanalysen und regelmäßige Evaluierung der IT-Sicherheitsstrategie
- 🌐 Einführung von Zugangskontrollsystemen, Verschlüsselungstechnologien und Sicherheitsüberprüfungen von Drittanbietern
- 🌐 Erstellung und Pflege von Notfall- und Wiederherstellungsplänen
- 🌐 Einbindung externer Dienstleister (Cloud, Logistik, Wartung) in das Risikomanagement

Die Meldepflichten bei Sicherheitsvorfällen sind gestuft: Innerhalb von 24 Stunden ist eine Erstmeldung zu erstatten, nach 72 Stunden ein Zwischenbericht, spätestens nach einem Monat ein Abschlussbericht.

Führen Sie frühzeitig ein Informationssicherheits-Managementsystem (ISMS) ein – auch wenn Ihr Unternehmen formal nicht direkt betroffen ist. Ein ISMS hilft Ihnen, Ihre Risikolage systematisch zu erfassen, Lieferantenbeziehungen vertraglich abzusichern und im Fall eines Kundenaudits nachweisbare Compliance vorweisen zu können. Nutzen Sie dafür anerkannte Normen wie ISO/IEC 27001 als Orientierungsrahmen.

Managementverantwortung und Sanktionen: Persönliche Haftung der Geschäftsführung

Die NIS-2-Richtlinie verankert die Verantwortung für Cybersicherheit ausdrücklich auf Ebene der Unternehmensleitung. Geschäftsführende Organe sind verpflichtet, die Einhaltung der Sicherheitsvorgaben aktiv zu überwachen, sich regelmäßig zu IT-Sicherheitsthemen fortzubilden und interne Kontrollmechanismen einzurichten. Bei grober Fahrlässigkeit oder unterlassener Aufsicht haften Geschäftsführer **persönlich**.

Das geplante Sanktionsregime ist gestaffelt: Bei besonders gravierenden Verstößen drohen Bußgelder in Millionenhöhe. Das BSI erhält erweiterte Befugnisse – darunter das Recht auf Vor-Ort-Prüfungen, die Anordnung von Sicherheitsmaßnahmen und die öffentliche Bekanntmachung von Sicherheitsmängeln.

Handlungsempfehlungen für Ihr Unternehmen

Prüfen Sie Ihren Status: Bewerten Sie anhand der NIS-2-Sektoren und der gesetzlichen Schwellenwerte (Umsatz, Mitarbeiterzahl), ob Ihr Unternehmen direkt betroffen ist. Analysieren Sie gleichzeitig Ihre Lieferkette: Sind Sie wesentlicher Lieferant für eine regulierte Einrichtung?

Erhöhen Sie Ihr IT-Sicherheitsniveau: Führen Sie ein ISMS ein, erstellen Sie einen Notfallplan und etablieren Sie technische Maßnahmen wie Backup-Strategien, Verschlüsselung und sichere Kommunikation.

Sichern Sie Ihre Lieferantenbeziehungen vertraglich ab: Passen Sie Ihre Verträge mit IT-Dienstleistern und Cloud-Anbietern an und dokumentieren Sie die Risikoklassifizierung Ihrer Lieferanten im ISMS.

Bereiten Sie Meldeprozesse vor: Definieren Sie interne Prozesse zur Erkennung und Meldung von Sicherheitsvorfällen, schulen Sie Ihre Mitarbeitenden und legen Sie klare Zuständigkeiten fest.

„Sie haben eine inhaltliche Frage oder einen Themenwunsch? Kein Problem! Schreiben Sie mir gern an redaktion@zolex.de Ich freue mich, von Ihnen zu hören.“



Holger Schmidbaur

KURZMELDUNGEN

Zollbewilligungen ab Juni 2026: Welche Daten Sie jetzt liefern müssen

Stellen Sie sich vor, der nächste Termin für die Überwachung Ihrer zollrechtlichen Bewilligung steht an. Sie reichen wie gewohnt Ihre Unterlagen ein, doch plötzlich fordert der Zoll Daten an, die Sie bisher nicht auf dem Schirm hatten. Ein reibungsloser Ablauf sieht anders aus und das kostet wertvolle Zeit im Tagesgeschäft.

Seit dem 1.6.2026 gelten neue Vorgaben für zollrechtliche Bewilligungen. Für neue Anträge und laufendes Monitoring müssen Sie zwingend die aktuelle Fassung des Fragebogens nutzen. Die bewährte Struktur bleibt bestehen und umfasst weiterhin alle relevanten Bereiche von Hinweisen über Unternehmensdaten bis zu Sicherheitsanforderungen. Wichtig: Bereits laufende Verfahren werden nach den bisherigen Vorgaben fortgeführt, sodass hier keine Umstellung nötig ist.

Die entscheidende Neuerung: So erfüllen Sie die neuen Anforderungen nach Art. 24 UZK-DVO präzise

Die Identifikation verantwortlicher Personen wird verschärft: Nach Art. 24 UZK-DVO müssen bei den meisten Bewilligungen künftig Steuer-ID und zuständiges Finanzamt angegeben werden, um Transparenz und Compliance zu stärken. Eine Ausnahme bleibt: Bei Fragebögen im laufenden Monitoring entfällt die Angabe vorerst weiterhin.

Abläufe anpassen: So koordinieren Sie die bereichsübergreifende Umsetzung im Unternehmen

Um die neuen Vorgaben der Zollverwaltung umzusetzen, arbeiten Sie eng mit anderen Bereichen zusammen. Die Personalabteilung liefert die Steuer-ID-Daten der verantwortlichen Personen, während die IT sichere Speicherlösungen in den

Systemen einrichtet. Vertrieb und Logistik prüfen parallel, ob bestehende Bewilligungen angepasst werden müssen oder neue Anträge erforderlich werden.

- 🌐 Abteilung Personal: Erheben Sie die Steueridentifikationsnummern der für die Zollbelange verantwortlichen Personen unter Einhaltung des Datenschutzes.
- 🌐 Abteilung IT: Implementieren Sie Zugriffsbeschränkungen für die neu zu erfassenden Steuer-ID-Daten in den betroffenen Systemen.
- 🌐 Zollverantwortliche: Überprüfen Sie bei jedem neuen Antrag, ob die aktuelle Fassung des Fragebogens vorliegt, und pflegen Sie die neuen Pflichtangaben ein.



FAZIT

Die Überarbeitung des Fragebogens erfordert eine Anpassung Ihrer internen Datenerfassung und gute Zusammenarbeit. Nutzen Sie die Übergangsregelungen im Monitoring, um Ihre Prozesse geordnet auf die neue Pflicht zur Steuer-ID-Angabe umzustellen und in allen Zollthemen rechtssicher zu bleiben.

Autor: Holger Schmidbaur

Nutzen Sie alle Vorteile Ihres Onlinebereichs!



Mehr als 200 Arbeitshilfen, Mustervorlagen, Checklisten als Download unter www.zolex.de/arbeitshilfen



Webinare und Veranstaltungen



Ausgaben-Archiv, inkl. Index und Spezialreports



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

