Darüber hinaus hat der Vorschlag COM 2016/616 keine direkten Auswirkungen auf die nationalen Beschränkungen gemäß AWV für die Ausfuhr von Rüstungstechnologie im Sinne von Position 0022 des Teils 1 A der AL sowie die Möglichkeit der Inanspruchnahme etwaiger Vereinfachungen, sodass für den Transfer von Rüstungstechnologie innerhalb eines Unternehmens oder eines Konzerns bis auf Weiteres die derzeit geltenden hohen Anforderungen bestehen bleiben.

Quellen und weiterführende Hinweise:

- Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über eine Unionsregelung für die Kontrolle der Ausfuhr, der Verbringung, der Vermittlung, der technischen Unterstützung und der Durchfuhr betreffend Güter mit doppeltem Verwendungszweck (Neufassung) vom 28.9.2016 (COM 2016/616).
- BAFA, Merkblatt Technologietransfer und Non-Proliferation, Stand: Juni 2016.
- BAFA, Merkblatt Sammelgenehmigungen für Rüstungsgüter, Stand: 29.6.2015.
- BAFA, Merkblatt zu Allgemeinen Genehmigungen und den diesbezüglichen Register- und Meldeverfahren, Teil I, Stand: Juni 2012.
- Tervooren/Mrozek in: Wolffgang/Simonsen/Rogmann, AWR-Kommentar, 42. EL, Ordnungs-Nr. 122, Art. 2 EG Dual-Use VO, Rn. 28 ff.
- Pietsch, Leitgedanken zur Exportkontrolle im Zusammenhang mit Cloud Computing und Fragen zu Cyberwar, in: Ehlers/Wolffgang, Recht der Exportkontrolle – Bestandsaufnahme und Perspektiven, S. 527 ff.
- Haellmigk, (Cloud-)Datentransfer und Exportkontrolle – Neue Compliance-Herausforderungen für Unternehmen, in: CCZ 2016, S. 31 ff. m.W.N.

Der „human security"-Ansatz der neuen Dual-Use-Verordnung: Neue Prüfpflichten für die Unternehmen

Die aktuelle Reform der Dual-Use-Verordnung und ihr Fokus auf die verwendungsbezogene Exportkontrolle – praktische Konsequenzen für die innerbetriebliche Exportkontrolle

Der Autor Dr. Philip Haellmigk, LL.M. ist Inhaber der internationalen Kanzlei HAELLMIGK, die auf die Bereiche Außenhandel, Exportkontrolle, Compliance und Vertragsrecht spezialisiert ist. Herr Dr. Haellmigk ist als Rechtsanwalt in Deutschland sowie in England (Solicitor of England and Wales) zugelassen. Zudem hat Herr Dr. Haellmigk einen Abschluss der französischen Rechtswissenschaften (Licence en Droit).

Die EU-Kommission hat am 28. September 2016 einen Vorschlag für eine Neufassung der Dual-Use-Verordnung veröffentlicht, der eine grundlegende Modernisierung des europäischen Exportkontrollsystems vorsieht. Ziel dieser Reform ist zum einen die Harmonisierung und Vereinfachung der europäischen Exportkontrollvorgaben. Zugleich wird aber auch eine Verschärfung der Exportkontrolle im Hinblick auf den Schutz von Menschenrechten („human security") angestrebt. Damit will die EU-Kommission insbesondere der Gefahr der ungehinderten Verbreitung von Überwachungstechnologie, die für Menschenrechtsverletzungen eingesetzt werden kann, begegnen und dadurch zugleich auch die digitale Infrastruktur der EU besser schützen. Der Vorschlag der EU-Kommission setzt dieses Ziel auf zwei Ebenen um: durch die Neudefinition des Begriffs „Dual-Use-Gut" sowie durch die Erweiterung der bisherigen Catch-All Kontrollen. Damit rückt die verwendungsbezogene Exportkontrolle immer stärker in den Vordergrund. Vorliegender Beitrag untersucht daher Inhalt und Umfang dieser neuen Kontroll-Vorgaben und geht dabei auch der Frage nach, welche praktischen Konsequenzen dieser neue menschenrechtsbasierte Ansatz der europäischen Exportkontrolle auf die Internal Compliance Programme der Unternehmen hat.

INHALT

Hintergrund des Kommissionsvorschlags

Am 28. September 2016 hat die EU-Kommission ihren Vorschlag zur Modernisierung des europäischen Exportkontrollsystems veröffentlicht.

Auch wenn dieser Vorschlag bereits das Ergebnis eines intensiven Abstimmungsprozesses mit den Verbänden und nationalen Verwaltungen der Mitgliedstaaten in den vergangenen Jahren

ist, ist er nur der erste Schritt im Rahmen des europäischen Gesetzgebungsverfahrens unter Einbeziehung des Europäischen Parlaments und des Rats der Europäischen Union, denen der Vorschlag bereits zugeleitet worden ist.

Während des Gesetzgebungsverfahrens steht die EU-Kommission zudem im Wege eines Dialogs mit der Zivilgesellschaft im engen Austausch mit der Industrie und ihren Interessensvertretern und veranstaltet hierzu Diskussionsforen (letztmalig am 12. Dezember 2016).

Das Verfahren wird voraussichtlich 1,5 Jahre dauern, so dass die Neufassung der Dual-Use-Verordnung zum Frühjahr 2018 in Kraft treten könnte.

Selbstverständlich kann der Vorschlag in diesem Zeitraum noch Änderungen erfahren. Gleichwohl ist die Richtung und Zielsetzung der Reform klar.

Zielsetzung des Kommissionsvorschlags

Die Modernisierung des europäischen Exportkontrollrechts verfolgt zwei Ziele:

Auf der einen Seite die Harmonisierung und Vereinfachung der Regelungen für die Exporte von Dual-Use-Gütern, auf der anderen Seite aber auch die Verschärfung der Ausfuhrkontrollen für bestimmte Güter und Technologien, die zwar zivilen Zwecken dienen, aber auch für Menschenrechtsverletzungen eingesetzt werden können.

Der Fokus dieser neuen Kontrollen gilt dabei vorrangig der Überwachungstechnologie. Aufgrund der aktuellen politischen Entwicklungen in bestimmten Regionen der Welt zeigt sich die EU-Kommission besorgt, dass gerade die Überwachungstechnologie (systematisch) für die Verletzung von Menschenrechten missbraucht werden könnte.

Diesen Bedenken begegnet die Kommission in ihrem Vorschlag durch ein zweistufiges Konzept:

- Einführung des Guts „Cyber-Überwachungstechnologie“ als neues Dual-Use-Gut;
- Erweiterung des Anwendungsbereichs der Catch-All Kontrollen.

Cyber-Überwachungstechnologie als neues Dual-Use-Gut

Nach dem bisherigen Verständnis ist ein Dual-Use-Gut ein Gut, das sowohl für zivile als auch für militärische Zwecke genutzt werden kann. Von dieser Definition rückt der neue Entwurf nun ab.

Nach dem Entwurf der neuen Dual-Use-Verordnung ist vom Begriff „Dual-Use-Gut“ auch Cyber-Überwachungstechnologie umfasst, die zur Begehung von schweren Menschenrechtsverletzungen oder des internationalen humanitären Rechts eingesetzt werden kann oder eine Gefahr für die internationale Sicherheit oder die wesentlichen Sicherheitsinteressen der EU und ihrer Mitgliedsstaaten darstellt (Art. 2 Abs. 1 b) des Verordnungsentwurfs). Der Begriff „Cyber-Überwachungstechnologie“ ist in Art. 2 Abs. 21 des Verordnungsentwurfs definiert: Cyber-Überwachungstechnologie umfasst Güter, die besonders konstruiert sind, um ein verstecktes Eindringen in Informations- und Kommunikationssysteme zu ermöglichen mit dem Ziel, Daten zu überwachen, zu sammeln und auszuwerten und/oder das angegriffene System lahmzulegen oder zu beschädigen. Hierzu zählen unter anderem Güter im Zusammenhang mit Mobilfunküberwachungstechnik, Intrusions Software, Überwachungszentralen, Lawful Interception- und Vorratsspeicherungssysteme sowie digitale Forensik.

Im Vergleich zu den vorherigen Entwurfsfassungen der neuen Dual-Use-Verordnung ist die Liste der in Art. 2 Abs. 21 des Verordnungsentwurfs aufgeführten Güter der Cyber-Überwachungstechnologie reduziert worden. Bestimmte Technologien wie Biometrie, Ortungsgeräte, Deep Packet Inspection Systeme sind von der Liste gestrichen worden. Da die Liste aber nur beispielhaft Technologien aufzählt und damit erkennbar nicht abschließend ist, ist der Anwendungsbereich dieser Regelung dadurch nicht eingegrenzt. Zudem können diese Technologien auch durch die neuen Catch-All Kontrollen erfasst werden (siehe unten).

Die Einfügung von „Cyber-Überwachungstechnologie“ ist kein völlig neuer Schritt der europäischen Exportkontrolle, da zahlreiche der genannten Technologien – auf Grundlage des von den EU-Mitgliedstaaten unterzeichneten Wassenaar Abkommens – bereits in Anhang I der Dual-Use-Verordnung (Kategorie 5) gelistet sind (Bsp: Intrusion Software, Mobilfunküberwachungstechnik).

Die Technologien, die tatsächlich neu in den Anhang I der neuen Dual-Use-Verordnung eingefügt werden, finden sich in der neuen Kategorie 10 des Anhang I („Andere Güter der Überwachungstechnologie“). Sie betreffen bestimmte Überwachungssysteme, Ausrüstung und Bestandteile für Informations- und Komunikationstechnik für öffentliche Netzwerke, deren Bestimmungsziel außerhalb des Zollgebiets der EU liegt und auch nicht die Länder Australien, Kanada, Island, Japan, Neuseeland, Norwegen, die Schweiz, Lichtenstein oder die USA betrifft (siehe Anhang II, Teil 2 der neuen Dual-Use-Verordnung).

Diese neuen Güter einschließlich hierfür besonders konstruierte Software und Technologie sind sehr spezielle Produkte und werden zumeist nur von Strafverfolgungsbehörden und Nachrichtendiensten verwendet. Insofern dürfte die Ausdehnung des Begriffs „Dual-Use-Gut“ für die Mehrzahl der Unternehmen in Deutschland und der EU zu keinen erhöhten innerbetrieblichen Exportkontrollen führen.

Gleichwohl stellt sich für die in dieser Branche tätigen Unternehmen und damit die grundsätzliche wettbewerbliche Frage, ob es sinnvoll und geboten ist, dass die EU – über die Güterliste des Wassenaar Abkommens hinausgehend – einseitig neue Güter als genehmigungspflichtige Dual-Use Güter listet.

Darüber hinaus mag eine erhöhte Kontrolle derartiger Technologien, insbesondere der Sicherheitstechnologien, ihren effektiven Gebrauch im Notfall gefährden.

So warnte die Industrie im Rahmen der Konsultationen über die Aufnahme von Intrusion Software in die Güterliste des Wassenaar Abkommens davor, dass im Falle von Cyber-Angriffen ein effektiver, d.h. unmittelbarer Einsatz von legaler Computersicherheitstechnik zur Abwehr der Cyber-Angriffe infolge einer Genehmigungspflichtigkeit derartiger Software stark eingeschränkt sein könne.

Hinweis:

In den USA sind die Bedenken der Industrie hierzu berücksichtigt worden. So hat das Bureau of Industry and Security (BIS) – nachdem die Intrusion Software in die Güterliste des Wassenaar Abkommens im Dezember 2013 aufgenommen worden

war – zwar einen Regelungsvorschlag zur Umsetzung in das nationale Exportkontrollrecht unterbreitet. Nach Stellungnahme und Kritik der US-amerikanischen Industrie ist die Regelung aber bislang nicht in Kraft getreten. Vielmehr haben die USA im Frühjahr 2016 erklärt, dass sie darauf drängen würden, die Intrusion Software und die hierfür erforderliche Technologie wie Hardware (teilweise) wieder von der Güterliste des Wassenaar Abkommens zu streichen.

Erweiterung des Anwendungsbereichs der Catch-All Kontrollen

Catch-All Kontrollen sind eine Auffangregelung für die nationalen Genehmigungsbehörden. Sie ermöglichen ihnen, Güter zu kontrollieren, die (noch) nicht als gelistete Dual-Use-Güter klassifiziert werden können, aber für bestimmte kritische Verwendungszwecke genutzt werden können. Die Catch-All Kontrollen sind ein – zumindest aus gesetzgeberischer und behördlicher Sicht – sinnvolles Instrument der Exportkontrolle gerade in Zeiten großer politischer und technischer Veränderungen. Für Unternehmen hingegen bedeuten sie erhöhten Compliance-Aufwand und größere Rechtsunsicherheit.

Nach aktueller Rechtslage unterliegt auch die Ausfuhr von nicht gelisteten Dual-Use-Gütern einer Exportkontrolle, wenn sie verwendet werden sollen oder können

- im Zusammenhang mit chemischen, biologischen Waffen oder Kernwaffen oder sonstigen Kernsprengkörpern oder entsprechenden Flugkörpern;
- für eine militärische Endverwendung und das Käufer- oder Bestimmungsland einem Waffenembargo unterliegt;
- als Bestandteile für Militärgüter im Sinne der nationalen Militärliste, die zuvor illegal aus einem EU-Mitgliedstaat exportiert wurden (Art. 4 Abs. 1–3 der Dual-Use-Verordnung).

Die Gehnehmigungspflicht wird ausgelöst, wenn die zuständige Behörde den Exporteur über die vebotene Verwendungsabsicht bzw. -möglichkeit informiert hat. Gleiches gilt, wenn dem Exporteur die verbotene Verwendungsabsicht bekannt ist. In diesem Fall hat er die zuständige Genehmigungsbehörde hierüber zu unterrichten, die dann über die Genehmigung des beabsichtigten Exports entscheidet.

Nach dem neuen Verordnungs-Entwurf besteht eine Genehmigungspflicht auch in den Fällen, in denen die Güter verwendet werden sollen oder können

- durch Personen, die beteiligt sind an oder verantwortlich sind für schwere Menschenrechtsverletzungen oder der Verletzung internationalen humanitären Rechts im Zielland, in dem von den betreffenden öffentlichen internationalen Institutionen oder zuständigen europäischen oder nationalen Behörden festgestellte bewaffnete Konflikte oder interne Repressionen existieren, und es Hinweise gibt, dass der vorgesehene Endkunde dieses Gut oder ähnliche Güter für derartige schwere Verletzungen nutzen wird (Art. 4 Abs. 1 d) des Verordnungsentwurfs);
- im Zusammenhang mit terroristischen Handlungen (Art. 4 Abs. 1 e) des Verordnungsentwurfs).

Unklare Begrifflichkeiten

Die Einführung der beiden Kriterien „Menschenrechtsverletzungen“ und „terroristische Handlungen“ als weitere kritische Verwendungszwecke in die Catch-All Kontrollen ist kritisch zu sehen.

Selbstverständlich ist der außenpolitische Ansatz der Wahrung und des Schutzes der internationalen Menschenrechte zu begrüßen. Allerdings ist fraglich, ob die Exportkontrolle das richtige Instrument für die Menschenrechtspolitik der EU ist. Dies gilt umso mehr, wenn eine rechtssichere Umsetzung dieser Vorgaben für die Unternehmen kaum möglich ist.

Die beiden neuen Verwendungskriterien enthalten zahlreiche generische Begrifflichkeiten, die der Präzisierung und Erläuterung durch den europäischen Gesetzgeber bedürfen.

Wann wird ein Land zu einem Land, in dem bewaffnete Konflikte oder interne Repressionen im Sinne des Verordnungsentwurfs existieren? Wer sind die betreffenden öffentlichen internationalen Institutionen oder nationale oder europäische Behörden, die eine solche Feststellung vornehmen?

Es gibt aktuell zahlreiche internationale Organisationen, die die Menschenrechtslage in den einzelnen Ländern untersuchen (beispielsweise Human Rights Watch und Amnesty International). Es kann aber nicht die Aufgabe des Exportunternehmens sein, sich auf Grundlage dieser Bewertungen eine eigene Länderliste mit existierenden oder drohenden Menschenrechtsverletzungen zusammenzustellen.

Das Gleiche gilt für den Begriff der schweren Menschenrechtsverletzung. Welche Menschenrechtsverletzungen sind damit gemeint? Klar ist, dass die Menschenrechte „Recht auf Leben“ und „Folterverbot“ davon umfasst sind, da diese Rechte bereits von den anderen Exportkontrollregularien (wie beispielsweise der Anti-Folter-Verordnung) erfasst sind. Vor dem Hintergrund der dem Verordnungsentwurf vorangegangenen Diskussionen ist davon auszugehen, dass der Fokus dieser neuen Catch-All Kontrolle auf der Meinungs- und Gedankenfreiheit liegt. Was ist aber beispielsweise mit dem „Recht auf ein faires Verfahren“? Wird dieses Menschenrecht tatsächlich (besser) geschützt, wenn der Export von nicht gelisteten Dual-Use-Gütern strengeren Kontrollen unterliegt?

Schließlich ist auch die Catch-All Kontrolle für terroristische Handlungen schwer zu fassen. Auch hier ist die gesetzgeberische Absicht, diese Verwendung ebenfalls zu berücksichtigen, grundsätzlich begrüßenswert. Es bleibt allerdings unklar, wann eine terroristische Handlung im Einzelnen vorliegt. Der Verordnungsentwurf verweist in Art. 2 Abs. 23 auf die Definition in Art. 1 Abs. 3 des Gemeinsamen Standpunktes 2001/931/GASP über die Anwendung besonderer Maßnahmen zur Bekämpfung des Terrorismus. Allerdings ist die dortige Definition einer terroristischen Handlung eher politischer als rechtlicher Natur („Bevölkerung einschüchtern“, „die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Landes destabilisieren oder zerstören“) und hilft nur bedingt bei der rechtssicheren Eingrenzung dieses Begriffs.

Welcher Sorgfaltsmaßstab gilt bei der Prüfung der Catch-All Kontrollen?

Die Erweiterung des Anwendungsbereichs der Catch-All Kontrollen geht einher mit der Verschärfung der Prüfpflichten der Exportunternehmen. Eine

Unterrichtungspflicht besteht im Gegensatz zur aktuellen Rechtslage nicht nur bei Kenntnis des Exporteurs („wissen“) hinsichtlich des kritischen Verwendungszwecks, sondern bereits dann, wenn der Exporteur bei Anwendung der bestehenden Sorgfaltspflichten Kenntnis erlangen kann („hätte wissen können“).

Hinweis:

Eine ähnliche Regelung enthält die Allgemeine Genehmigung Nr. EU002 (Teil 3 Nr. 2); siehe Anhang II b der Dual-Use-Verordnung.

Jedoch wird nicht konkretisiert, welchen Sorgfaltsmaßstab der Ausführer anlegen muss, um der Unterrichtungspflicht gegenüber der Genehmigungsbehörde zu genügen. Es ist davon auszugehen, dass bereits der begründete Verdacht einer verbotenen Verwendungsabsicht der nicht gelisteten Dual-Use Güter im Zielland zu einer Unterrichtungspflicht führt.

Die neuen Catch-All Kontrollen müssen präzisiert werden

Ohne präzise gesetzgeberische oder behördliche Handlungsweisungen und -empfehlungen zu den neuen Catch-All Kontrollen würden die Exportunternehmen bei der Umsetzung dieser Regelungen alleingelassen.

Sie müssten aus ihrer Sicht (und damit rein subjektiv) zutreffende Beurteilungsparameter entwickeln und in ihre Exportabwicklungsprozesse einfügen in der Hoffnung, dass sie hiermit die neuen Regelungen hinreichend beachten und die Behörden ihre Einschätzung auch teilen werden.

Zudem wäre eine Integration dieser neuen Catch-All Kontrollen ohne nähere Erläuterung der einzelnen Prüfschritte in automatisierte Exportabwicklungsprozesse so nicht möglich. Eine manuelle Einzelprüfung ist für die meisten Unternehmen aufgrund ihres Exportvolumens faktisch nicht realisierbar.

Zum Zwecke der Rechts- wie Planungssicherheit für die Unternehmen müssen die Behörden diese neuen kritischen Verwendungszwecke daher näher definieren. Dies kann auf verschiedene Weise geschehen: entweder durch eine eindeutige Beschreibung der Gefahrenlage, durch eine Auflistung kritischer Länder (Black List), durch eine Aufzählung unkritischer Länder (White List) und/oder durch eine Liste an kritischen Gütern.

Anhand dieser Parameter kann das Exportunternehmen – zumindest besser – entscheiden, ob es das beabsichtigte Exportgeschäft tatsächlich durchführen möchte oder ob der zu erwartende Compliance-Aufwand den Ertrag aus dem Exportgeschäft übersteigt. Zudem erleichtern diese Einschränkungen auch eine angemessene vertragsrechtliche Absicherung für den Fall eines kritischen Endkunden bzw. einer kritischen Endverwendung im Sinne der neuen Catch-All Kontrollen.

Hinweis:

In § 9 AWV wird die Catch-All Kontrolle durch produkt- und länderspezifische Parameter eingegrenzt.

Auch die Exportkontrollsysteme außereuropäischer Länder kennen derartige Hilfestellungen im Bereich der Catch-All Kontrollen. So gibt es beispielsweise im japanischen Exportkontrollrecht die sogenannte Commodity Watch List, die Güter aufführt, bei denen eine (hohe) Wahrscheinlichkeit besteht, dass sie für die Herstellung von Massenvernichtungswaffen verwendet werden.

Fazit

Infolge des neuen „human security“-Ansatzes des aktuellen Vorschlags zur Modernisierung der Dual-Use-Verordnung werden die Anforderungen an die verwendungsbezogene Exportkontrolle deutlich erhöht. Die Verschärfung der Prüfung erfolgt durch die Ausdehnung des Begriffs „Dual-Use-Gut“ auf Cyber-Überwachungstechnologie sowie durch die Erweiterung der Catch-All Kontrollen auf die etwaige Verwendung des Guts für Menschenrechtsverletzungen und terroristische Handlungen im Zielland

Zwar mögen sich die jetzigen Regelungsvorschläge bis zum voraussichtlichen Inkrafttreten der neuen Dual-Use-Verordnung im Frühjahr 2018 in ihren Formulierungen an der ein oder anderen Stelle ändern. Die Richtung und Zielsetzung der Reform wird jedoch beibehalten werden. Die Unternehmen müssen sich also darauf einstellen, dass sich der administrative Prüfungsaufwand für ihre Exportgeschäfte erhöhen wird und die bestehenden Internal Compliance Programme einschließlich der Vertragsdokumente angepasst werden müssen. Zu hoffen ist, dass der europäische Gesetzgeber den Unternehmen mithilfe von klaren Handlungsanweisungen und Empfehlungen bei der Umsetzung und Anwendung dieser neuen Regelungen hilft!

Quellen und weiterführende Hinweise:

Proposal for a Regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast) – 2016/0295(COD).