Cyber-Security und Exportkontrolle

5. November 2020

Die Digitalisierung des weltweiten Handels nimmt immer weiter zu. Laut einem Bericht des Handelsblatts werden im 21. Jahrhundert Daten zum wichtigsten Handelsgut. Die fortschreitende Entwicklung der 3D-Drucktechnologie ermöglicht es, statt der Güter Datensätze zu versenden, mit deren Hilfe Waren vor Ort gedruckt werden. Je mehr die Digitalisierung des Handels voranschreitet, desto wichtiger werden Cyber-Security-Produkte.

Was vielen Unternehmern nicht bekannt ist: Bereits das Hochladen von Konstruktionsplänen in die Cloud, deren Bereitstellung auf einem Server oder der Transfer von (Cyber-Security-)Software können der staatlichen Exportkontrolle unterliegen. Das kann zum einen zur Folge haben, dass auch Unternehmen die Exportkontrolle beachten müssen, die bislang nicht damit befasst waren. Zum anderen müssen auch „klassische" Exportunternehmen ihr Exportkontrollsystem auf die Ausfuhr von Technologie und Software erweitern.

Hintergrund

Ein zentrales Ziel der Exportkontrolle ist es, eine Bedrohung Deutschlands oder seiner Bündnispartner durch konventionelle Waffen, Massenvernichtungswaffen sowie Gütern, die sowohl für zivile als auch potentiell militärische Zwecke Verwendung finden können (*Dual-Use-Güter*), zu verhindern. Verstärkt gehen Gesetzesvorhaben noch auf eine andere Absicht zurück: Nach einem Reformvorschlag der Europäischen Union sollen Exportkontrollen vermehrt zum Schutz von Menschenrechten beitragen.

In beiden Fällen führt die gestiegene und steigende Relevanz der Cyber-Security zu einem Wandel der jeweiligen Bedrohungsszenarien und Gefahrenlagen. Software kann mittlerweile das Schadenspotential von konventionellen Waffen übertreffen. Zudem können Überwachungstechnologien in autokratischen Staaten dazu genutzt werden, Menschenrechtsverletzungen zu begehen. Daher steht der Handel mit cybersicherheitsrelevanter Software immer mehr im Fokus der Exportkontrolle.

Die veränderte tatsächliche Bedrohungslage führt konsequenterweise auch zu einer Veränderung des rechtlichen Rahmens staatlicher Exportkontrolle wie zuletzt durch Anpassung des Anhangs I der Verordnung EG Nr. 428/2009 (*Dual-Use-Verordnung*) mit Wirkung zum 31. Dezember 2019. Der europäische Gesetzgeber hat dabei an seiner im Jahr 2018 getroffenen Entscheidung festgehalten, die Offenlegung von Sicherheitslücken und die Reaktion auf Cybervorfälle zur Verfügung gestellten Technologien von der Exportkontrolle auszunehmen. Damit fällt nach wie vor die Ermittlung, Meldung oder Mitteilung einer Sicherheitslücke an Einzelpersonen oder

Organisationen oder der Austausch der erforderlichen Informationen über einen Cybersicherheitsvorfall aus dem Anwendungsbereich der Exportkontrolle.

Grundzüge der Exportkontrolle

Grundsätzlich ist der Export von Waren frei. Die staatliche Exportkontrolle beschränkt diese Freiheit und unterscheidet zwischen verbotenen, genehmigungsbedürftigen und meldepflichtigen Transaktionen. Verboten ist eine Transaktion z.B. bei einem personen- oder länderbezogenen Embargo. Der Exporteur benötigt eine Ausfuhrgenehmigung insbesondere dann, wenn das Gut, die Software oder die Technologie in Anhang I der Dual-Use-Verordnung oder in der militärischen Ausfuhrliste gelistet ist. Dafür müssen die Eigenschaften des jeweiligen Produkts mit dem in der Liste genannten abgeglichen werden.

Eine entscheidende Ausnahme besteht jedoch nach Art. 4 Abs. 4 der Dual-Use-Verordnung. Dieser knüpft nicht an die Eigenschaft an, sondern an die beabsichtigte Verwendung. Nach dieser sog. „catch all" Klausel kann auch die Ausfuhr von Gütern, Softwaren oder Technologie, die nicht explizit gelistet sind, genehmigungsbedürftig sein. Das ist dann der Fall, wenn dem Ausführer bekannt ist, dass das auszuführende Produkt einer kontrollwürdigen Verwendung zugeführt werden soll (z.B. die Verwendung in Massenvernichtungswaffen). Es wird an dieser Stelle von dem Ausführer erwartet, dass dieser die ihm oder allgemein verfügbaren Informationen aufbereitet und bewertet.

Eine Ausfuhr ohne Genehmigung kann für die verantwortlichen Personen eine Straftat oder Ordnungswidrigkeit darstellen. Im Fall einer vorsätzlichen Ausfuhr ohne Genehmigung droht eine Gefängnisstrafe bis zu 5 Jahren oder eine Geldstrafe (§ 18 Abs. 2 AWG). Im Fall einer fahrlässigen Begehung liegt eine Ordnungswidrigkeit vor. Sie kann mit einer Geldbuße von bis zu 500.000 Euro festgesetzt werden – pro Ausfuhr (§ 19 AWG). Verantwortliche Personen sind das Management und die für die in der Exportkontrolle tätigen Personen. Aber auch das Unternehmen kann mit einer Geldbuße von bis zu 10 Millionen Euro belegt werden (§ 30 OWiG).

Die Reichweite staatlicher Exportkontrolle am Beispiel von Software

Die Ausfuhr von Software ist nach derzeitiger Rechtslage vereinfacht gesagt dann genehmigungsbedürftig, wenn die Software in besonderem Zusammenhang zu der Verwendung eines genehmigungsbedürftigen physischen Gutes steht oder ihr bereits ein eigenständiges Gefahrenpotential zukommt. Letzteres kann beispielsweise dann der Fall sein, wenn die zu exportierende Software modifizierbare Verschlüsselungstechnologie enthält. Derartige Kryptographie wird auch für den Betrieb autonomen Fahrens eingesetzt. In Kanada unterliegen daher der Export dieser Verschlüsselungstechnologien, die technischen Mittel, um diese zu erzeugen und die auf autonomes Fahren ausgelegten Fahrzeuge selbst der Exportkontrolle. Vor dem Hintergrund des sog. Cyber-Warfare und den darin enthaltenen Bedrohungsszenarien für Deutschland

und seine Bündnispartner kann darüber hinaus jegliche Software der Exportkontrolle unterfallen, soweit sie auch militärisch genutzt werden kann. Zum Beispiel kann eine Software, die ein Kraftwerk im Notfall zum Ausschalten zwingt, auch zur Vorbereitung eines militärischen Angriffs dienen.

Im Gegensatz zur Ausfuhr von konventionellen Gütern ist bei der Ausfuhr von Software nicht nur das physische Verbringen ins Ausland entscheidend. Auch der immaterielle Verkehr durch elektronische Medien ist erfasst. Für cloudbasierte Software-Anwendungen bedeutet das, dass jeder Upload von Daten in die Cloud außerhalb der Europäischen Union und jede Einräumung von Zugriffsmöglichkeiten für Nicht-EU-Angehörige – auch wenn der Server in Deutschland steht – nach Auffassung der Behörden einen prinzipiell genehmigungsbedürftigen Ausfuhrvorgang darstellen kann. Das gilt auch für die Zugriffsmöglichkeiten innerhalb desselben Konzerns. Es kommt bei der Ausfuhr von Software im Übrigen auch nicht auf den Wert der jeweiligen Transaktion an.

Die Notwendigkeit unternehmensinterner Vorsorgemaßnahmen

Mit Blick auf das durchaus empfindliche Sanktionsregime des Außenwirtschaftsrechts sollten Unternehmen, die mit Cyber-Security Produkten handeln, intern überprüfen, inwieweit sie der Exportkontrolle unterliegen. Gegebenenfalls muss ein adäquates Exportkontrollsystem geschaffen werden. Wie weit die Aufbereitung und Verwertung verfügbarer Information gehen muss, um die tatsächliche Verwendung des Produkts im Ausland zu bewerten, hängt vom jeweiligen Einzelfall ab. Die diskutierte Reform der Dual-Use-Verordnung zum verstärkten Schutz der Menschenrechte könnte zu weitreichenden Nachforschungspflichten und weitergehender Haftung für die verantwortlichen Personen führen. So betont der Rat in seinem aktuellen Änderungsvorschlag u.a. die Wichtigkeit der Ausfuhrkontrolle auch in Bezug auf nichtgelistete Dual-Use-Überwachungstechnologie und -software (Erwägungsgrund 5). Auch ist eine Harmonisierung der Kontrolle der Erbringung von technischer Unterstützung bei sensiblen Gütern vorgesehen (Erwägungsgrund 11), die über bestehende Genehmigungserfordernisse hinauszugehen vermag. Wie die Reform der Dual-Use-Verordnung jedoch konkret aussehen wird, ist weiterhin unklar.

Fazit

Die Ausweitung staatlicher Exportkontrolle unter dem Schlagwort der Cyber-Security ist in weiten Teilen der Veränderung tatsächlicher Bedrohungslagen geschuldet. Kehrseite dieser Entwicklung ist, dass auch solche Unternehmen von der Exportkontrolle umfasst sind, die bislang ohne Berührungspunkte zum Außenwirtschaftsrecht arbeiteten. Sie sehen sich somit besonderen rechtlichen Herausforderungen ausgesetzt. In der Regel werden sie ein funktionierendes Exportkontrollsystem einführen müssen.

BLOMSTEIN wird die weiteren Entwicklungen beobachten und darüber informieren. Wenn Sie Fragen zu den potenziellen Auswirkungen der Cyber-Security auf Ihr Unternehmen oder Ihre Branche haben, stehen Ihnen Dr. Roland M. Stein und Dr. Leonard von Rummel jederzeit gern zur Verfügung.