Software mit US-Open-Source-Komponenten

Wenn ein Software-Hersteller auch US-Software-Komponenten verwendet, stellt sich die Frage, ob er auch das US-Exportrecht beachten muss und welche Folgen dies hat. Vor allem bei der Nutzung von US-Open-Source-Software-Komponenten bestehen erhebliche Unklarheiten, ob dies zu US-Genehmigungspflichten führen kann.

PD Dr. Harald Hohmann
Rechtsanwalt,
Hohmann Rechtsanwälte

info@hohmann-rechtsanwaelte.com
www.hohmann-rechtsanwaelte.com

Ausgangsfall: D in Deutschland stellt eine Software her, die einen sicheren Zugang zu Benutzerkonten gestatten soll. Hierfür ist Kryptografie (Verschlüsselungstechnologie) notwendig. D entwickelt keine eigene Kryptografie; stattdessen greift D auf eine Vielzahl von US-Open-Source-Software-Komponenten zu. Die meisten dieser Komponenten sind auf 5D002 gelistet. D ermöglicht den grenzüberschreitenden Download seiner Software.

D möchte wissen: Ergeben sich Exportbeschränkungen aus dem EU-Exportrecht? Und falls diese Software dem US-Exportrecht unterfallen sollte: Welche Beschränkungen ergeben sich aus dem US-Exportrecht?

Beschränkungen nach EU-Exportrecht

Indem D grenzüberschreitend den Download seiner Software ermöglicht, liegt eine „Ausfuhr" vor. Hierfür muss das EU-Exportrecht beachtet werden. Mangels Anhaltspunkten für eine sensitive Verwendung geht es um die Frage, ob die Software von D gelistet ist. Angenommen, D weiß nicht, ob seine Software gelistet ist: Dass D keine eigene Kryptografie entwickelt, sondern dass auf US-Open-Source(OS)-Software zugreift, schließt nicht aus, die Software gelistet sein könnte, und zwar v.a. unter Kategorie 5 Teil 2 (Kryptografie). Sofern keine der zahlreichen Ausnahmen zu dieser Listenposition greift, dürfte sie im Zweifel von 5D002 erfasst sein; diese Vermutung ergibt sich aus der US-Listung. Dann würde D für den grenzüberschreitenden Download dieser Software eine BAFA-Genehmigung benötigen.

US-Exportrecht anwendbar?

US-Exportrecht wäre dann anwendbar, wenn einer der folgenden sechs „US-Türöffner" hier greift: (1) US-Territorium, (2) US-Personen, (3) Güter *made in the USA*, (4) Güter *made in Europe* mit US-Komponenten von mehr als minimalem US-Wertanteil, (5) direkte Produkte aus US-Technologie oder (6) USD-Geschäfte oder US-Sekundär-Sanktionen (vgl. unseren Beitrag in ExportManager 4/2019).

Am naheliegendsten ist hier, dass es um den „US-Türöffner" Nr. 4 geht: Güter *made in Europe* mit US-Komponenten von mehr als minimalem US-Wertanteil. Die US-Wertanteilsgrenze für die US-Komponenten liegt bei 25%; nur für eine Ausfuhr in vier Terrorunterstützer-Staaten (Iran, Kuba, Nordkorea, Syrien) läge sie bei 10% (so zumindest nach den EAR = *Export Administration Regulations*; OFAC-Regulations für Embargos sehen z.T. geringere Wertgrenzen vor). Da hier auf eine Vielzahl von US-OS-Komponenten zugegriffen wird, ist nicht ausgeschlossen, dass diese Wertgrenze hier überschritten wird (im Streitfall muss dies geprüft werden). Daher ist hier US-Exportrecht im Zweifel anwendbar.

©Pixels Hunter/Shutterstock

Für IT-Unternehmen kann eine US-Genehmigungspflicht für die Ausfuhr von Software greifen.

US-Genehmigungspflicht für Ausfuhr dieser Software?

Nach General Prohibition 2 würde eine Genehmigungspflicht nur dann bestehen, wenn hier vier Voraussetzungen erfüllt sind:

1. In die deutsche Software von D wurde „kontrollierte" US-Software inkorporiert oder gebündelt.

2. Die De-Minimis-Grenze wird überschritten.

3. Der Kontrollzweck hinter der Listung der US-Komponenten ist sensitiv für das Endbestimmungsland.

4. Die US-Software muss Gegenstand der EAR-Jurisdiktion sein.

Zu den Voraussetzungen 1 bis 3 der US-Genehmigungspflicht

Zu 1.: Eine „Inkorporierung" liegt dann vor, wenn die US-Software wesentlich ist für das Funktionieren der Software von D, wenn die US-Software üblicherweise im Verkauf der Software von D enthalten ist und wenn sie zusammen mit der Software von D reexportiert wird. Bei der Software von D dürfte dies vorliegen, sodass eine „Inkorporierung" vorliegt. Es handelt sich um „kontrollierte" US-Software, weil diese von 5D002 gelistet ist.

Zu 2.: Es soll davon ausgegangen werden, dass die De-Minimis-Grenze von i.d.R. 25% hier überschritten wird.

Zu 3.: Der Kontrollzweck hinter 5D002 ist NS1 (*National Security 1*) und AT1 (*Anti-Terrorism 1*). AT1 ist nur sensitiv für die genannten vier Terrorunterstützer-Länder. Hingegen ist NS1 sensitiv für alle Länder der Welt außer Kanada. Damit ist der Kontrollzweck hinter der Listung der US-OS-Software sensitiv für alle Länder der Welt (außer Kanada).

Zur Voraussetzung 4 („Gegenstand der EAR-Jurisdiktion") bei Open-Source-Software

Bei US-OS-Software ist es fraglich, ob sie Gegenstand der EAR-Jurisdiktion ist, v.a. dann, wenn sie veröffentlicht wurde und für die Allgemeinheit zugänglich ist, ohne dass Restriktionen für ihre Verbreitung bestehen. Für Verschlüsselungsquellcodes, die auf 5D002 gelistet sind, gibt es zwei Tests, die kumulativ erfüllt sein müssen, damit der Quellcode nicht „Gegenstand der EAR-Jurisdiktion" ist:

- Test 1: Der Quellcode ist „öffentlich zugänglich", weil er veröffentlicht ist und keine Restriktionen für seine weitere Verbreitung bestehen.

- Test 2: Der Quellcode implementiert eine Standard-Verschlüsselung, die öffentlich zugänglich ist (Alternative 1) oder: Er implementiert eine Nicht-Standard-Verschlüsselung, zu der eine E-Mail-Notifizierung an das Bureau of Industry and Security (BIS) hinzukommt (Alternative 2).

Es wird angenommen, dass die Voraussetzungen von Test 1 hier vorliegen. Zu Test 2 gibt es Unsicherheiten, wann eine „Standard-Verschlüsselung" vorliegt. Einige meinen, dass es ausreichen dürfte, wenn die Verschlüsselung durch eine US-Standardisierungseinrichtung erfolgt. Andere meinen, dass hierfür eine Anerkennung durch internationale Standardisierungseinrichtungen (wie ITU, ISO etc.) erforderlich ist. Wenn man die Definition von „Nicht-Standard-Verschlüsselung" in § 772.1 EAR berücksichtigt, dürfte eine Standard-Verschlüsselung eine veröffentliche Verschlüsselung sein, die auch internationalen Standards entspricht.

Sollte allein eine Anerkennung durch US-Standardisierungsgremien vorliegen, muss vertieft weiter geprüft werden, ob schon eine Standard-Verschlüsselung bejaht werden kann. Falls keine Standard-Verschlüsselung vorliegen sollte, muss der Software-Hersteller eine E-Mail-Notifizierung an das BIS vornehmen, um zu erreichen, dass für den Export seiner Software keine US-Genehmigungspflicht (für alle Länder außer Kanada) ausgelöst wird. Bei einer öffentlich zugänglichen Standard-Verschlüsselung würde hingegen keine solche US-Genehmigungspflicht ausgelöst.

Resümee

Software-Häuser meinen häufig, sie könnten unbegrenzt auf US-Open-Source-Software zugreifen, ohne dass hierbei eine US-Genehmigungspflicht für die Ausfuhr der Software greift. Die Nutzung von US-OS-Software kann erstens dazu führen, dass US-Exportrecht hier anwendbar ist, und zweitens auch dazu, dass dies bei Re-Exporten eine US-Genehmigungspflicht auslöst. Sollte nämlich wider Erwarten keine Standard-Verschlüsselung vorliegen, würde die Notwendigkeit einer US-Genehmigung (für Re-Exporte in alle Länder der Welt außer Kanada) nur dann entfallen, wenn vorher eine E-Mail-Notifizierung an das BIS erfolgt ist.

Und für die Abgrenzung Standard- gegen Nicht-Standard-Verschlüsselung sind Untersuchungen anzustellen, wie etwa folgende: Haben nur US- oder auch internationale Standardisierungseinrichtungen die Verschlüsselung anerkannt? Gibt es umfassenden Urheberschutz mit aufwendigen Lizenzierungsbedingungen für die Software? Bereits die Prüfung, ob die US-Software die De-Minimis-Schwelle überschreitet, erfordert aufwendige Prüfungen. Software-Hersteller sollten diese Anforderungen des US-Exportrechts beachten, um einen US-Exportverstoß zu vermeiden. ◄

Wegen aktueller Hinweise zum EU-Exportrecht vgl. HIER *und zum US-Exportrecht vgl.* HIER