Digitization 4.0 – compliance challenges under EU sanctions

A closer look: dos and don’ts when providing technology and software in sanctioned countries

By Dr. Alexander Cappel

Introduction

The world of law currently faces various legal issues caused by digitization of business streams. Those legal topics include numerous IP questions (ownership of big data, protection of know-how, IP protection of 3D printing, scope of copyright protection, standard essential patents), antitrust and liability-related risk allocation as well as topics concerning technology export control and EU sanctions. In upcoming editions of Business Law Magazine, we will deal with a number of these topics. In this edition, we will take a closer look at the challenges companies face with EU sanctions if technology and software is provided to sanctioned countries.

The majority of EU sanctions stipulate prohibitions on making funds or economic resources available either directly or indirectly to certain listed individuals and legal entities (economic-resource embargo). The various EU sanctions specify that the term "economic resource" (see, for example, Article 1 [h] of Council Regulation [EU] No. 267/2012 dated March 23, 2012, concerning restrictive measures against Iran according to which "economic resources" means assets of every kind, whether tangible or intangible, movable or immovable, which are not funds, but which may be used to obtain funds, goods or services) has to be interpreted broadly and, thus, it generally covers not only the delivery of goods to certain customers designated by all EU sanctions, but also the provision of specific technology or software. With this in mind, the German Federal Office for Economic Affairs and Export Control (Bundesamt für Wirtschaft und Ausfuhrkontrolle, BAFA) has also issued guidance on this issue, stating that, in particular, embargos targeting certain listed individuals and legal entities will have to be considered prior to any exports of technology and software (see page 10 of the BAFA guidance on the transfer of technology and nonproliferation: link as of April 29, 2016). As a result, companies providing technology or software are obliged to both scrutinize – in the same way companies exporting, for instance, industrial goods must do so – the respective technology or software against applicable export restrictions and check their customers and business partners against the various EU sanction lists under which individuals or legal entities might be designated. As an even more challenging consequence, companies are also required to ensure that planned...
business transactions will not lead to indirect breaches of EU sanctions because, for example, an unlisted business partner is owned or controlled by a listed individual or company.

Against this background, companies dealing with technology and software should not only focus their compliance systems on potential export restrictions in terms of specific technology and software, but also focus on customer and business-partner due-diligence measures. This article will examine feasible approaches to potential business-partner due-diligence measures to comply with applicable EU sanctions, especially with regard to the export of technology and software that might pose further specific risks and challenges.

**Scope of the economic-resource embargos**

EU sanctions (for example, against Russia or Iran) entail differing restrictions on, inter alia, the free movement of goods, technologies and services including financial services. Almost all EU sanctions stipulate, however, prohibitions on making funds or economic resources available either directly or indirectly to certain sanctioned individuals or legal entities. According to the German Federal Supreme Court (Bundesgerichtshof, BGH) jurisprudence, funds or economic resources will be deemed to have been “made available” once a sanctioned individual or legal entity gains factual control over such funds or economic resources (see BGH, April 23, 2010, AK 2/10, published in NJW 2010, page 2,370 et seq.).

With regard to technology or software, an even stricter standard might apply since, for example, Article 2, paragraph 2, subparagraph iii of EC Dual Use Regulation 428/2009 stipulates that technology will be considered to have been “exported” upon “transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the European Community.” This also applies to “oral transmission of technology when the technology is described over the telephone.” Since there is, at least under German law, no relevant case law available, there is a risk that companies might, under certain circumstances, be obliged to conduct enhanced business-partner checks as early in the process as oral contract negotiations when background information regarding certain technology or software will be orally transmitted (for example, over the telephone). This may ultimately lead to having to increase compliance efforts since companies may be required to check their business partners long before they ultimately enter into a business relationship.

**Companies dealing with technology and software should not only focus their compliance systems on potential export restrictions, but also focus on customer and business-partner due-diligence measures.**

Moreover, it is important to note that making funds or economic resources available to an unlisted company that is owned or controlled by a sanctioned individual or company may also constitute a breach of the economic-resource embargo since in this case the transmitted technology or software (as an economic resource) may indirectly benefit a listed company (for more information, see chapter five “Embargo- und Sanktionsmaßnahmen” by Marian Niestedt in EU-Außenwirtschafts- und Zollrecht, 2014). In this regard, an unlisted company is considered owned by a listed target if the relevant company or individual holds more than 50% of its shares. In contrast, an unlisted company is deemed to be controlled by a sanctioned target if such a sanctioned target exercises factual control over the unlisted company due to special voting rights, specific agreements with other shareholders or any other means. By inverse conclusion, any mere minority shareholding by a listed individual or company in an otherwise unlisted company to which funds or economic resources is to be made available will not necessarily present a breach of the EU sanctions. The specific circumstances do, however, have to be analyzed in each case prior to executing the business (or even prior to entering into contractual negotiations) in order to avoid a breach of the economic-resource embargo. According to “Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy” dated April 30, 2013 (EU guidelines), in particular, (a) any contractual links between the unlisted company and the sanctioned target will have to be considered as well as (b) the relevance of the affected area of operations to the listed company and the goods’ properties and (c) the characteristics of the funds or economic resources made available, including their potential practical use by, and ease of transfer to,
the listed company (see link as of April 29, 2016).

As a result, the prohibition on making funds or economic resources directly or indirectly available to certain individuals or entities on the EU sanctions list poses an exceptional compliance challenge. This is particularly the case since EU sanctions themselves do not comprise detailed provisions outlining the scope of exactly what compliance obligations need to be heeded. It is important to note that violations of EU sanctions, including violations of the economic-resource embargo, may result in administrative and even criminal-law penalties not only against the involved companies but also against the acting individuals. According to the administrative and criminal-law provisions for violations of EU sanctions stipulated in the German Foreign Trade Act (Außenwirtschaftsgesetz), any individuals contravening economic-resource embargos must, at the very least, have acted in negligence before they face administrative or criminal repercussions. Furthermore, the EU sanctions specify that acting parties may not be held liable if they had no knowledge nor reason to assume, that any of their actions would violate provisions of the economic-resource embargo. This means the compliance challenge companies generally face is identifying the due-diligence measures they have to conduct in order to not be held liable in the unfortunate event that a violation of EU sanctions may later be discovered (that is, because technology was indeed delivered indirectly to a sanctions target although the prior due-diligence measures did not discover it from an ex ante perspective).

**Risk-based approach to due diligence for sanctions**

Since neither German nor EU lawmakers provide clear guidance on the extent to which business partners need to be checked in terms of EU sanctions, in particular, in terms of the economic-resource embargo, a risk-based approach seems to be advisable to minimize liability risks as much as possible. Although there is no one-size-fits-all approach, a risk-based approach should generally contain the following elements:

**Risk classification of (potential) customers**

On the basis of their regional center of operations as well as on other circumstances that may be cause for concern, (potential) customers should be categorized as “high risk,” “moderate risk” or “low risk.” Parameters for the classifications may comprise the following:

- In particular, for cases where the (potential) customer or business partner is located in a country against which sanctions are enforced (for example, Iran, Russia or Syria) or where obvious indications are given that the (potential) customer or business partner directly operates with such a country, increased caution should be exercised in reviewing the business relationship. As a result, the customer or business partner is to be classified as high risk.

- Similarly, for cases where the (potential) customer or business partner is located in a classic “gateway country” (for example, the United Arab Emirates or Iran), such business relationships may also be classified as high risk if additional circumstances suggest a connection to a company or individual in a sanctioned country exists (for example, obvious shareholding connections or business relationships in sanctioned countries). Otherwise, those (potential) customers or business partners may be classified as “moderate risk.”

- In contrast, a (potential) customer or business partner located in a country other than those mentioned above, may, in the absence of further risk-increasing factors, be classified as “low risk.”

**Identification of due-diligence measures**

In addition to risk classification, potential due-diligence measures should be developed for each category. The following due-diligence measures may be feasible, although the individual circumstances always have to be borne in mind:

- No matter what the category – high risk, moderate risk or low risk – every known customer or business partner as well as all other involved parties should be routinely checked against the applicable sanctions lists in order to identify if the business involves any listed persons or entities.

- In particular with regard to high-risk and moderate-risk customers and business partners, companies may also want to conduct risk-based background researches (for example, by conducting Internet research, using special tools or databases and instructing local lawyers or business consultancies) and/or obtain disclosure of the ownership structure.
from the (potential) customer or business partner.

- Especially with regard to high-risk customers or business partners, companies may want to also obtain written assurances that the technology or software will not be made available to the benefit of any designated targets. Various international companies have also made it a best practice to include provisions in their business contracts (in particular with high-risk customers) that prohibit clients from further disposing of received goods to sanctioned targets within the applicable legal framework. With regard to these two measures, companies should carefully consider if they are permitted under local law to conduct them or if and to which extent anti-boycott legislation (such as Section 7 of the German Foreign Trade Order [Außenwirtschaftsverordnung]) may apply.

**Summary**

Companies dealing with technology and software generally have routinely implemented compliance measures to address the respective export restrictions stipulated for technology and software in the EC Dual Use Regulation 428/2009 and the Export List (see link as of April 29, 2016) published by BAFA. In addition to those export restrictions, however, EU sanctions pose further compliance challenges to those companies because technology and software may be affected by the economic-resource embargos stipulated by almost all EU sanctions.

**EU sanctions pose further compliance challenges to those companies because technology and software may be affected by the economic-resource embargos stipulated by almost all EU sanctions.**

EU sanctions do not, however, provide clear guidance on what compliance measures need to be fulfilled in order to not be held liable. As a result, companies should implement their due-diligence measures using a risk-based approach as no standardized measures apply. Although such measures should generally safeguard against violations of EU sanctions occurring, enhanced caution must, in particular, be applied to cases where a company indicates that a minority shareholder of a (potential or existing) customer is on the EU sanctions list. In those cases, authorities and courts may argue that EU sanctions were indirectly breached (that is, the technology was delivered indirectly to a listed target).

Since breaches against EU sanctions may lead to severe criminal and administrative penalties – not only against the involved company but also against the responsible individuals – as well as cause considerable loss of reputation, companies dealing with technology and software – along with other exporting companies – should carefully consider whether pursuing business opportunities in sanctioned countries justifies the investment of resources necessary to ensure compliance with EU sanctions. Companies that do not do this could face severe criminal-law liabilities.

---

Dr. Alexander Cappel  
Rechtsanwalt, Counsel  
Clifford Chance Deutschland LLP  
Frankfurt am Main  
alexander.cappel@cliffordchance.com  

www.cliffordchance.com