Rödl & Partner

NEWSLETTER SANCTIONS

SUCCESSFUL TOGETHER

Issue:
February
2024

The latest news on EU sanctions against Russia and Belarus

www.roedl.com | www.roedl.de

Rödl & Partner

NEWSLETTER SANCTIONS

SUCCESSFUL TOGETHER

Issue: February 2024

Read in this issue:

→ Current EU sanctions issues after the 13th sanctions package

As the second anniversary of Russia's invasion of Ukraine has come, the European Commission on 21st of February announced that EU has agreed on the 13th sanctions package against Russia. The following measures to be adopted:

- 2000 new entities and individuals to be added to a sanctions list
- More Russian companies to be banned from purchasing dual-use goods from EU companies (Annex IV of Council Regulation (EU) No 833/2014)
- New restrictions on drones supply to Russia
- No new measures on certain economic sectors to be imposed
- No new import bans which most likely are expected to come up later with the 14th sanctions package

Following the implementation of the 12th sanctions package, which was adopted less than two months ago, companies should currently keep an eye on the following sanctions issues:

Software exports bans

As per adopted Council Regulation (EU) 2023/2878 of 18 December 2023 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, the existing prohibition on the provision of services which is stated in Article 5n of Council Regulation (EU) No 833/2014 extended in a way to also include the prohibition to sell, supply, transfer, export, or provide, directly or indirectly, software for the management of enterprises and software for industrial design and manufacture as listed in Annex XXXIX of Council Regulation (EU) No 833/2014 to the Government of Russia or legal persons, entities or bodies established in Russia.

The new Annex XXXIX of Council Regulation (EU) No 833/2014 indicates exact software which falls under the restrictions:

1. Software for the management of enterprises, i.e. systems that digitally represent and steer all processes happening in an enterprise, including:

- Enterprise resource planning (ERP)
- Customer relationship management (CRM)
- Business intelligence (BI)
- Supply chain management (SCM)
- Enterprise data warehouse (EDW)
- Computerized maintenance management system (CMMS)
- Project management software
- Product lifecycle management (PLM)
- Typical components of the above-mentioned suites, including software for accounting, fleet management, logistics and human resources

2. Design and Manufacturing Software used in the areas of architecture, engineering, construction, manufacturing, media, education and entertainment, including:

- building information modelling (BIM)
- computer aided design (CAD)
- computer-aided manufacturing (CAM)
- engineer to order (ETO)
- typical components of above-mentioned suites

No-Russia contractual clause

Council Decision (CFSP) 2023/2874 requires that exporters contractually prohibit re-exportation to Russia and re-exportation for use in Russia of sensitive goods and technology as listed in Annexes XI, XX and XXXV to Regulation (EU) No 833/2014, common high priority items, or firearms and ammunition as listed in Annex I to Regulation (EU) No 258/2012.

The following legal conditions must be met according to the Article 12g of Council Regulation (EU) No 833/2014:

- When selling, supplying, transferring or exporting to a third country, with the exception of part-

ner countries listed in Annex VIII to this Regulation, goods or technology as listed in Annexes XI, XX and XXXV to this Regulation, common high priority items as listed in Annex XL to this Regulation, or firearms and ammunition as listed in Annex I to Regulation (EU) No 258/2012, exporters shall, as of 20 March 2024, contractually prohibit re-exportation to Russia and re-exportation for use in Russia
- The above requirement shall not apply to the execution of contracts concluded before 19 December 2023 until 20 December 2024 or until their expiry date, whichever is earlier
- The exporters shall ensure that the agreement with the third-country counterpart contains adequate remedies in the event of a breach of a contractual obligation (No Russia clause)
- If the third-country counterpart breaches any of the contractual obligations (No Russia clause), exporters shall inform the competent authority of the Member State where they are resident or established as soon as they become aware of the breach

The following goods and technologies fall under the No-Russia contractual clause:

- Aircraft, spacecraft, and parts thereof as listed in Annex XI of Council Regulation (EU) No 833/2014
- Jet fuel and fuel additives as listed in Annex XX of Council Regulation (EU) No 833/2014
- Firearms and other arms as listed in Annex XXXV of Council Regulation (EU) No 833/2014
- Common high priority items, e.g., 8542.31 Electronic integrated circuits, as listed in the new Annex XL of Council Regulation (EU) No 833/2014
- Firearms, their parts and essential components and ammunition as listed in Annex I to Council Regulation (EU) No 258/2012

The contractual prohibition of selling, supplying, transferring or exporting to a third country is not applicable for partner countries listed in Annex VIII of Council Regulation (EU) No 833/2014:

- USA
- Japan
- UK
- South Korea
- Australia
- Canada
- New Zealand
- Norway
- Switzerland

Updated FAQs

On February, European Commission updated the Consolidated FAQs on the implementation of Council Regulation No 833/2014 and Council Regulation No 269/2014 regarding the above mentioned software ban. What could be important is that the prohibition to sale, supply, transfer, export, and the provision of the software listed in Annex XXXIX also covers software updates. Also, assistance or advice relating to software updates and upgrade, as well as bespoke software updates and upgrades were already subject to a prohibition to provide IT Consultancy services to the Russian Government or Russian entities, according to Article 5n(2). In addition, the intention of Article 5n(2b) is to deprive the Government of Russia and legal persons, entities or bodies established in Russia of the latest software development. The prohibition in Article 5n(2b) does not affect the sale, supply, transfer, export, and the provision of the software in question to entities in other third countries, which are not targeted by the provision. However, it is also a crucial part that EU operators must carry out relevant due-diligence to avoid participating in circumvention.

Also, other important FAQs which were updated are related to these topics:

- Public procurement
- Oil price cap
- Transit of listed goods via Russia
- Imports, purchase and transfer of listed goods
- Divestment from Russia
- Restrictions on diamonds
- Export-related restrictions for dual-use goods and advanced technologies
- State-owned enterprises
- Russian Central Bank

Since the end of last year (2023) until now, European Commission also issued new official guidance which are covered by the below sanctions topics:

- Price Cap Coalition statements and guidance
- Guidance on firewalls
- List of economically critical goods
- List of common high priority items
- Guidance on due diligence
- Guidance on stopped goods

For any assistance in solving difficult sanctions related topics please contact our Sanctions Compliance Team of Rödl & Partner. Our professionals will provide you legal sanctions risk assessment, including sanctions screening of your business partners.

Contact for further information

Ignas Tamašauskas
Senior Compliance Consultant
T +370 5 2123 590
ignas.tamasauskas@roedl.com

→ Sanction issues in M&A practice – update on DD requirements and transaction design

In the past, sanctions usually only played an incidental role in transactions, in the sense that compliance with sanctions was covered by the standard formulation of the guarantee catalog, according to which the target company carries out its business activities in accordance with the applicable legal requirements.

Only in the case of more or less obvious points of contact with countries that were the subject of sanctions (in particular Iran, Belarus and, from 2014, Russia) was compliance with applicable sanctions increasingly also explicitly demanded as an assurance.

However, with Russia's attack on Ukraine and the subsequent rapid escalation of sanctions packages by the EU, US, UK and other countries and organizations, the issue of sanctions compliance has become a core topic of due diligence and a frequently decisive element of transaction structure and acquisition contract design.

One of the main reasons for this is that sanctions issues are of (possibly even existential) importance both at the level of the target company and at the level of those directly involved in the transaction, such as buyers, sellers and other parties such as investors, financing banks, W&I insurance companies, etc.

And yet the issue of sanctions is still not a matter of course for many economic players, especially in (apparently) only national transactions. Occasionally one is even confronted with a denial-approach, stating that sanctions regulations merely create "red-tape" whose non-compliance would not have any tangible negative consequences.

Such an impression can indeed arise, as the consequences of sanction violations are not yet visible to the public in their full extent. Occasionally, there are media reports about particularly obvious sanctions violations and circumvention measures, which at least result in corresponding reputational damage for the actors concerned. However, the criminal consequences associated with violations of EU (and national) sanctions will only become visible in the media in a few years' time – once the investigations, indictments and convictions have been concluded. The competencies and personnel capacities required for the expected large number of proceedings have been created in Germany, in particular through the Second Sanctions Enforcement Act, the creation of the Central Office for Sanctions Enforcement, the Federal Financial Criminal Police Office and the FIU (Financial Intelligence Unit). It is therefore assumed that a tsunami-like wave of corresponding proceedings is currently building up.

Some of the current and immediate consequences of sanctions violations or inadequate sanctions compliance measures are still hidden from public view – but are clearly visible in our consulting practice.

Banks in particular play a prominent role here. They are the ones who, through their compliance departments, which are highly sensitized by strict regulations on money laundering and combating terrorism, also uncover indirect sanctions violations – for example through subsidiaries in third countries. The declarations and evidence of internal sanctions compliance measures, process documentation and responsibilities required against the background of the KYC documentation requirements and the necessary risk assessment make banks the key drivers in the enforcement of EU and, in particular, US sanctions requirements.

In contrast to the consequences under criminal law, the reactions on the part of banks are swift and the consequences are directly noticeable for companies. These generally consist of the threat and subsequent implementation of account freezes, account terminations and the termination

of financing agreements. It is therefore important to be prepared and react correctly to corresponding notifications and requests from banks due to the short response times given.

Especially in M&A transactions, it is important to adapt to the changed requirements. Sanctions law issues must be considered throughout almost the entire course of a transaction, both on the acquirer's and the seller's side. To this end, the existing due diligence obligations for the parties involved must be individually determined in advance and suitable risk management methods applied.

It is therefore important to carry out checks on the target company, the companies and natural persons involved as early as the initial contact or the initiation of talks. The focus here is in particular on clarifying any possible entry of the persons directly involved in the transaction as well as the other persons along the shareholding structures through to the beneficial owners on a relevant sanctions list.

The extent of the requirements arising from the applicable due diligence obligations must be assessed on the basis of the risk factors to be determined for the specific case.

The same applies to the evaluation of the results of a sanctions list comparison. If, for example, it turns out that formally there is no exercise of control by persons subject to individual sanctions due to the shareholding ratio under company law (e.g. if the shareholding ratio is below 50 %), an examination of the shareholding history may nevertheless reveal indications that suggest a de facto control position of the sanctioned person. This would be the case, for example, if a transfer of shares to persons who are economically or personally dependent on the sanctioned person took place in connection with the inclusion in a sanctions list. If there are corresponding indications, further checks must be carried out, for example of articles of association, partnership agreements, voting agreements, trust agreements, etc.

Possible topics and subjects of sanctions audits in connection with transactions can be listed as follows:

1. Examination of applicable sanctions regimes.

- Determination of the applicable sanctions law / scope of application (EU – territorial principle / US sanctions OFAC/BIS, e.g. primary sanctions via US nexus – dollar as agreed currency for the purchase price, participation of persons with US citizenship or green card, banks with branches in the USA, goods of US origin)
- Application risk beyond the defined scope of application, e.g. extraterritorial application of US sanctions (secondary sanctions)

2. In accordance with the sanctions provisions identified as applicable, the following parties are then screened under individual sanctions law (Sanctioned Party List Screening)

- Target company (-ies)
- Transaction parties (up to UBO level)
- other persons directly and indirectly involved in the transaction (e.g. financing banks, investors, trustees, investment banks, brokers, W&I insurers)

3. DD review of the target company under sanctions law

- Compliance with sanctions regulations and possible risks and violations due to type of business activity / services and activities / production and trade of sanctioned goods / creation and use of circumvention structures
- Checking sanctions lists of senior employees (in case of suspicion)
- Sanctions list screening of business partners, customers and suppliers (using screening software that enables the comparison of large amounts of data)
- Fulfilment of compliance requirements in the form of export control and sanctions compliance systems (internal guidelines, process specifications, checklists, manuals, use of technical aids, responsibilities)
- Known sanctions violations, adverse media check
- Ongoing (investigative) proceedings against companies and private individuals involved (e.g. customs, law enforcement authorities – also in other countries)

Prior to a sanctions check, it is also advisable to clarify which requirements exist with regard to the scope and depth of the audit, evidence requirements, level of detail and documentation on the part of third parties, in particular W&I insurers and financing banks.

It is important for the seller to identify sanction-related weaknesses and risks in advance of the transaction (e.g. as part of a vendor DD) and to eliminate or at least minimize them prior to an acquisition review.

Where no clear results can be achieved due to the vagueness of sanctions law (in some cases intended by the legislator) or due to a lack of information, the parties involved often only have the option of carrying out and documenting a risk assessment and weighing up in accordance with the requirements, on the basis of which economic decisions can then be made.

The fact that such vagueness probably collides with the constitutional requirement of certainty in criminal law will certainly be a weighty argument in the future when defending against criminal prosecution of allegations of a sanctions violation.

Ultimately, however, the transaction-induced sanction check must be included in the overall view of compliance assessments. There are many overlaps here with measures that lead to the clarification and detection of breaches in other areas. A sanctions check should therefore be carried out in close coordination with experts from other compliance areas (e.g. KYC, CRA, fulfilment of investigation, documentation and reporting obligations in the area of AML, UBO investigation, forensic investigations) in order to avoid unnecessary duplication of audits. The underlying data and findings should be exchanged on an ongoing basis – with the aim of conducting a holistic risk assessment and identifying suitable measures for dealing with these risks.

These can consist, for example, of the carve-out of certain risk-exposed parts of the target company or the removal of units from the group to be acquired prior to the acquisition, for example in the form of the sale of shareholdings in subsidiaries in Russia or Belarus (if currently possible at all due to the Russian and Belarusian approval requirement for direct and indirect share transfers) or also of units in third countries with (suspected) participation in circumvention structures.

If the sanctions list comparison of the target company's master data has revealed that certain suppliers or customers are subject to a high risk of sanctions, the termination of business relationships with these persons should be made a condition precedent. The exclusion of exposed persons (e.g. if they have been involved in sanctions violations in the past or if their participation could establish a US nexus) is also an option to consider.

Deficits in the design and execution of internal compliance processes should preferably be remedied before the acquisition or the expenses required for this after the acquisition should be taken into account as a deduction item when determining the purchase price.

If specific sanction risks have been identified, the buyer should in general insist that the seller accepts indemnification for any financial losses that may arise as a result (including fines imposed on the company).

Investigation proceedings initiated between singing and closing or sanction violations dis-closed by the media should be covered by suitable MAC clauses.

Particularly in the area of sanctions, a documentary presentation that goes beyond mere red-flag reporting in the DD report is recommended in order to enable the buyer to exculpate itself for actions prior to the acquisition in the event of future criminal investigations.

When drafting the warranty and indemnification provisions, it should be noted that although W&I insurers require corresponding evidence of sanction risk assessments, they do not generally grant insurance cover for this area and the insurance contracts contain corresponding exclusion clauses.

The question of whether the acquirer is obliged under the so-called "public disclosure obligation" introduced with the 11th EU sanctions package pursuant to Art. 6b Regulation (EU) 833/2014 to notify the law enforcement authorities of any sanctions violations of the target company that come to its attention during the DD check is still unresolved. Attorneys in particular are explicitly excluded from such a notification obligation, which is subject to a fine, which is why consideration should be given to making the relevant infor-

mation available exclusively to the attorneys commissioned with a corresponding assessment (e.g. via a so-called clean team agreements) – in line with the usual procedure for the disclosure of sensitive information that falls under the restrictions of antitrust or data protection law.

For any assistance in solving difficult sanctions related topics please contact our Sanctions Compliance Team of Rödl & Partner. Our professionals will provide you legal sanctions risk assessment, including sanctions screening of your business partners.

Contact for further information

Tobias Kohler
Partner
T +370 5 212 3590
tobias.kohler@roedl.com

→ News flash: General authorisation for the provision of business software and services to Russian (subsidiary) companies

In brief

1. From 20 June 2024, business software and certain services may only be supplied to Russian companies that are 100% controlled by an EU parent company after prior notification to the Federal Office of Economics and Export Control (German *BAFA*).

2. The services concerned include:

- Provision of business management software (ERP software) and industrial design
- Auditing, accounting and tax consultancy, PR
- Legal and IT consultancy
- Market and opinion research
- All types of technical assistance and brokering services related to the above

3. With general authorisation No. 42 (General Authorisation) of 20 February 2024, BAFA has approved these services in general form. This means that an individual authorisation is no longer required, but only a single notification to BAFA no later than 30 days after the start of the service. The existing subsidiary privilege will continue to apply until 20 June 2024.

4. The General Authorization generally applies to German residents within the meaning of Section 2 (15) Foreign Trade and Payments Act (German *Außendwirtschaftsgesetz*). Thanks to the General Authorisation, a detailed and time-consuming authorisation procedure is no longer necessary.

In details

The EU's 12th sanctions package changed the requirements for the provision of services to Russian legal entities. Until then, a blanket exemption applied to the provision of services to subsidiaries under the 100 per cent control of one (or more) EU parent companies ("subsidiaries").

From 20 June 2024, the ban on the provision of services to Russian legal and natural persons would have applied to subsidiaries as well. In order to anticipate the expected flood of applications, BAFA has now responded with General Authorisation No. 42.

Accordingly, the services concerned are authorised in general form, so that a formal authorisation in individual cases pursuant to Article 5n (10) (c) and (h) of Regulation (EU) No. 833/2014 (Russia Embargo Regulation) is no longer required.

Requirements for notification to BAFA

The following aspects have to be considered when notifying BAFA

1. Formal notification

Anyone providing the above-mentioned services must register as a user via the BAFA online portal (ELAN-K2) before using the General Authorisation for the first time or within 30 days. Registration is required. The registration can either be made by the service provider itself or you can have Rödl & Partner authorised as a service provider so that the registration is made by us.

2. Content of the notification

The notification must contain information about the service provider, the service recipient and the company that controls or owns the service recipient. It is sufficient to report the first supply of services. Subsequent supplies of services to the same recipient do not need to be notified, even if they are different services.

In practice, the General Authorisation makes the work much easier: a time-consuming authorisation procedure and a detailed description of the services in each individual case are no longer necessary.

It should be noted, however, that the General Authorisation is granted on condition that the service providers actually submit the relevant notification to the BAFA. If they fail to do so, they will not be able to claim the General Authorisation. and the service will be prohibited under the Russia Embargo Regulation from 20 June 2024!

For any assistance in solving difficult sanctions related topics please contact our Sanctions Compliance Team of Rödl & Partner. Our professionals will provide you legal sanctions risk assessment, including sanctions screening of your business partners.

Contact for further information

Michael Manke
Associate Partner
Attorney-at-law
T +370 5 212 3590
michael.manke@roedl.com

Imprint

Publisher:
Rödl & Partner
www.roedl.com

Responsible for content:
Tobias Kohler
tobias.kohler@roedl.com

Ignas Tamašauskas
ignas.tamasauskas@roedl.com

Michael Manke
michael.manke@roedl.com