



European Commission

Guidance for EU

operators:

Implementing enhanced due diligence to shield against Russia sanctions circumvention

© European Union, 2023

Reuse is authorised provided the source is acknowledged. Distorting the original meaning or message of this document is not allowed. The European Commission is not liable for any consequence stemming from the reuse of this publication. The reuse policy of European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39).

For any use or reproduction of photos or other material that is not under the copyright of the European Union, permission must be sought directly from the copyright holders.

All images © European Union, 2023, except:

cover photo: © adhi megatama - stock.adobe.com

Introduction

The European Union has imposed unprecedented restrictive measures ('sanctions'¹) in response to Russia's war of aggression against Ukraine and the complicity of Belarus in it. One of the objectives of the sanctions is to weaken the Russian government's ability to finance its war.

Faced with the scale of the sanctions, Russian targets have consequently deployed various techniques to circumvent these measures, for instance by using complex financial schemes, falsifying the nature or origin of the goods traded or relying on the jurisdictions of third countries. Listed persons and entities have also made efforts to conceal their assets.

As a result, there is an increased risk that EU operators will find themselves in a position where they may facilitate prohibited activities involving Russia, thereby reducing the impact of the sanctions and possibly violating EU regulations. Such increased risk justifies the development of an enhanced due diligence model, in particular for high-risks sectors and complex supply chains.

EU operators incorporated or constituted under the law of an EU Member State are directly required to comply with EU sanctions law.

This guidance aims at providing a general overview of the main points of consideration for EU operators in view of their due-diligence work and is intended to support their compliance efforts. It is not meant to be an exhaustive document applicable to all sectors and types of EU operators. Depending on new circumvention patterns, the list of recommended due diligence measures will be updated accordingly. Current focus of the guidance are export related sanctions, however EU operators are expected to have due-diligence measures for all their relevant activities that might fall under the scope of EU sanctions.

In addition to this guidance, the Commission has published lists of sanctioned high-priority battlefield items² and economically critical goods³ to support due diligence and effective compliance by exporters and targeted anti-circumvention actions by customs and enforcement agencies of partner countries determined to prevent that their territories are being abused for circumvention of EU Russia sanctions purposes. Annex IV of the Council (EU) Regulation 833/2014 includes a list of entities in Russia and in certain third countries with close commercial or other links to the Russian military. This list has been periodically updated. Other jurisdictions publish similar information about entities that present higher risks of circumvention.

¹ [Overview of sanctions and related tools \(europa.eu\)](#)

² [List of High-Priority Battlefield items](#)

³ [Economically critical goods list](#)

Risk assessment of possible sanctions circumvention

EU operators should identify, assess, and understand the possible risks of circumvention, most relevant for their business activity and operational model and should take action to mitigate these risks. This should be carried out on a recurring basis, based on open sources information on the evolution of circumvention techniques. It should be noted that EU operators that set up transactions, rather than merely facilitate them, are in a better position to assess the risk and perform due diligence. In addition, depending on the nature of the transactions (e.g. commercial, export/import) the stakeholders in a position to detect sanctions circumvention may vary.

As stated in the European Commission's FAQs on Russian sanctions, *"EU operators have to perform appropriate due diligence calibrated according to the specificities of their business and the related risk exposure. It is for each operator to develop, implement, and routinely update an EU sanctions compliance programme that reflects their individual business models, geographic areas of operations and specificities and related risk-assessment regarding customers, business partners and staff."*⁴

To mitigate to the maximum extent their exposure to possible sanctions circumvention schemes, EU operators should conduct a strategic risk assessment, following these successive steps:

- I. Identification of threats and vulnerabilities:** Risk can be defined as the ability of a threatening agent to exploit a vulnerability. EU operators should stay alert to the main techniques used by Russian actors to circumvent sanctions, as well as to the emerging patterns. They should also map out the types of products, transactions and economic activities within their range of services that are at risk of being involved in Russian sanctions circumvention techniques (see 2b "Examples of typologies of sanctions circumventions").

Examples of who might be particularly impacted and need to exercise particular vigilance.

Example (1): An EU based manufacturer of semiconductor devices. It is well known that these goods are in high demand in Russia and their export to Russia from the EU is prohibited. The volume of exports is increasing towards third countries with which trade was previously limited or non-existent.

Example (2): An EU based manufacturer of items identified in the list of high-priority battlefield items. It is well known that battlefield items are in high demand in Russia and their export to Russia is subject to export restrictions from the EU.

Example (3): An EU based manufacturer of goods which have a very specific tariff classification and as such may or may not fall in the scope of the export ban.

Example (4): An EU based manufacturer of goods which may be often and easily miscategorised under an HS code not subject to sanctions.

Example (5): An EU based freight forwarder company that is organising the transport of the exported goods.

⁴ [FAQ - Circumvention and Due Diligence.pdf \(europa.eu\)](#)

- II. Risk analysis:** Operators should assess the nature of the risks to which their sector, products and economic activities are exposed to, and understand how those risks can materialise. To this end, they may use risk indicators, typologies and any other relevant information that is publicly available or forms part of their specialised knowledge.

Example (1):

- main risks identified: attempts of transferring goods to Russia via third countries;
- *how can the risks they be prevented:* enhanced evaluation of the risk by trained staff, monitoring of contractual arrangements for customers and business partners, ensuring the processing and end-use of the product.⁵

- III. Design of mitigating measures:** How can the risks be prevented? What are the measures to implement in order to mitigate these risks? Which are the relevant national authorities to raise operators' awareness of the risk and provide guidance?

- IV. Implementation of mitigating measures:** To mitigate the risk of circumvention, EU operators that identify higher risk areas in their business may proactively incorporate, as appropriate, the results of steps I1) and I3) into their internal risk management practices and procedures, and have controls in place to test the effective functioning of those procedures.

- V. Regular updating:** The evolution of circumvention techniques and the use of increasingly complex methods of circumvention require the mapping of threats and vulnerabilities is updated whenever necessary, for instance when sanctions are amended or new sanctions are adopted, and in any case on a regular basis. This requires that the operator has satisfactory procedures in place for following and updating maintaining the necessary information (e.g. sanctions legislation, circumvention techniques, circumvention trade flows) up-to-date. The training of the staff on these issues is of critical importance, as well. Moreover, it is recommended that senior management of a company is personally involved and informed regularly by company compliance officers on risks identified and measures taken.

By adopting a risk assessment and risk management approach to circumvention, EU operators will help ensure that measures taken to prevent or mitigate circumvention are commensurate with the risks identified.

The implementation of risk assessment and risk management should also enable EU operators to concentrate their efforts on the most sensitive cases and thus allocate their resources in the most effective way.

⁵ See Notice 3 on special clause in contracts [Notice 3 \(2022/C 145 I/01\)](#).

1. Enhanced due diligence

Although there is no single model for conducting due diligence, EU operators should, following the assessment of circumvention risks and typologies outlined in this guidance, align their efforts to comply with the risks identified. This risk assessment and risk management approach should lead EU operators to adopt a proportionate approach and, in particular, by placing focus on those sectors that are deemed to be most critically exposed to circumvention risks, and accordingly put in place adequate commensurate systems to prevent those risks from occurring ('enhanced due diligence').

a) General good practices

As stated in the European Commission's FAQs, *"There is no one-size-fits-all model of due diligence. It may depend – and be calibrated accordingly – on the business specificities and the related risk exposure. It is for each operator to develop, implement, and routinely update an EU sanctions compliance programme that reflects their individual business models, geographic and sectoral areas of operations and related risk assessment. Such sanctions compliance programmes can assist in detecting red flag transactions that can be indicative of a circumvention pattern⁶".*

Good practices can be adopted when implementing enhanced due diligence (e.g. when the EU operator's activity exposes him to a particular risk), at different levels:

On/at the stakeholders level (identification and verification of business partners, customers, their representatives, their beneficial owners and other possible persons of interest):

- Is there any proven business record?
- Is there any effort from the stakeholder to maintain sanctions internal control systems / ensure sanctions compliance?
- Who are the main stakeholders involved/relevant for my business?
- Are any of the direct stakeholders (customers, distributors, agents, etc.) or indirect stakeholders (end-user, intermediaries, banks etc.) targeted by EU sanctions? Do we know all stakeholders?
- If yes, did the stakeholder undergo changes in their ownership structure upon or after the adoption of sanctions? Was it set up or established after the introduction of the sanctions?
- Are these stakeholders affected by sanctions through ownership or control??
- Who is the end user? Can the end user certificate be provided?

⁶ [FAQ - Circumvention and Due Diligence.pdf \(europa.eu\)](#)

⁷ The EU can designate individuals and entities for an assets freeze or for specific restrictions such as ban on all transactions (e.g. art.5aa of Reg.833/2014). These measures can extend to non-designated entities as follows: (i) for the assets freeze measures, assets of entities owned for more than 50 % by the designated person/entity or controlled by them shall be frozen; (ii) specific restrictions applied to designated entities can extend to entities whose proprietary rights are directly or indirectly owned for more than 50 % by the designated entities.

On/at the transaction level, flows of money and route of goods, transportation companies' involvement and responsibility:

- What is the country of origin/transit/destination of the goods?
- What is the country of transit and of destination? Is this country neighbouring Russia or Belarus, has easy transport / access (i.e. passport/shipping controls) to Russia or Belarus, or otherwise known to re-export goods to those jurisdictions? Should the export be subject to enhanced vigilance/end-use controls?
- Are complex/unusual transportation routes being used?
- Has the value of goods changed since the imposition of sanctions? Has the method of trading/transacting changed, e.g. contract conditions imposed?
- What is the business rationale for the transaction? Does the transaction or shipment seem in line with expectations regarding the (prospective) customer from a business perspective? Or does the transaction or shipment seem unjustified from a business perspective?
- Does the transaction use complex financial schemes which are not justified by its purpose?
- Has the method of transport/shipping changed since the imposition of sanctions?
- Are there unusual or abnormal elements in the documentation that do not match (e.g. between financial and contract)?
- Any other red flag? (see below)

On the goods:

- Are the goods subject to any EU sanctions or export/import control rules?
- Are the goods included in the list of high-priority battlefield items or on the economically critical goods list?
- Do the goods contain components that are more likely to be disassembled and diverted for non-intended purposes?
- Are the goods similar to sanctioned ones? If the goods are shipped through Russia or Belarus, is the route standard and economically viable?
- Particular attention should be paid for exports to countries which do not apply restrictions on exports of sensitive goods to Russia and Belarus (see [notice of 1st April 2022](#)).

b) Best practices to address typologies of sanctions circumventions

Trade: preventing possible diversion to/from Russia and/or Belarus via third countries

EU operators should have in place adequate due diligence procedures to ensure that their operations that deal with sanctioned for Russia goods are not diverted to Russia.

First of all, in particular when exporting goods subject to restrictions, they need to know their counterparts and how reliable they are. They should include, in particular, contractual clauses with their third-country business partners prohibiting further re-exports of the items to Russia and Belarus, as well as possible ex post verifications. These clauses may take the form e.g. of a statement that the respect of such provision is an essential element of the contract, or of contractual clauses committing

the importer in third countries not to export the concerned goods to Russia or Belarus, and not to resell the concerned goods to any third party business partner that does make a commitment not to export the concerned goods to Russia or Belarus, which then give rise to liability in case the latter re-exports the items to those countries (see [notice to operators of 1st April 2022](#)). It is vital that the contractual clause is valid and can be enforced under the law applicable to the contract.

It is for Member States to implement and enforce sanctions. The Commission has the role of ensuring uniform implementation throughout the Union and monitoring enforcement by the Member States.

If a sanctioned item exported from the EU to a third country is re-exported as such to Russia, the competent authorities may consider the EU exporter's failure to conduct adequate due diligence as a violation of EU sanctions law. Any suspicious activity in the field of trade should be reported, in line with legal requirements, to the relevant national authority, such as financial intelligence units, customs and border authorities or relevant supervisory authority, if any.

Banking and Finance: enhanced vigilance with regard to the use of correspondent accounts

Transactions relying on correspondent accounts can lead to a higher residual risk of sanctions circumvention.

Correspondent accounts are relationships between financial institutions that facilitate the provision of services from one (the correspondent) to another (the respondent). These services can relate to transactions for the respondent financial institution itself or on behalf of its customers, including processing wire transfers, international trade settlements, remittances, and cross-border payments.

Financial institutions that maintain correspondent accounts for foreign financial institutions are required to establish appropriate, risk-based enhanced due diligence frameworks, with policies, procedures, and processes that are reasonably designed to assess and mitigate the risks inherent with these relationships.

In the context of sanctions implementation, financial institutions should monitor transactions related to correspondent accounts to detect and prevent potential attempts to breach sanctions. Without prejudice to Anti-Money-Laundering and Counter Financing of Terrorism (AML/CFT) requirements, their due diligence frameworks should take into account the level of risk of sanctions evasion posed by the foreign respondent.

The risks can vary depending on the respondent's profile. In practice, this means that financial institutions may conduct an adequate assessment of risks and appropriate due diligence of the risks present in:

- (1) the foreign respondent's business and markets;
- (2) the type, purpose and anticipated activity;
- (3) the nature and duration of the relationship with the foreign respondent; and
- (4) the supervisory regime of the jurisdiction in which the foreign respondent is licensed, and to design and implement controls to manage these risks effectively.

2. Circumvention red flags related to business partners and customers

Various indicators⁸ should alert EU operators when they enter into a commercial relationship with a new trading partner. When conducting general due diligence, if operators find evidence of any of the indicators below, they should launch a deeper screening.

- Indirect transactions (such as those using intermediaries, shell companies etc.) that make no or little economic sense;
- New customer / transactions with companies located in countries known as “circumvention hubs” and involving items listed as high-priority battlefield items.
- Transit through countries or territories known as “circumvention hubs” based on the information available. Specific measures that can be taken depending on the role and responsibility of the operator, e.g.:
 - exporter who uses an external transport company: checks regarding the type of means of transport use, routings, use of sub-contractors, etc.
 - transport company which is responsible for the transport of the cargo: checks regarding the actual goods to be transported; match with documentation, etc.
- Complex corporate or trust structures linked to countries friendly to Russia or whose complexity is not justified by the business profile of the customer. Use of trust arrangements or complex corporate structures involving offshore companies;
- Business partner has been recently established or has merged with a sanctioned entity or an entity linked to sanctioned entities or persons;
- Business partner shares address with multiple different companies (e.g., it is likely a shelf company);
- Changes of ownership of a corporate holding to reduce ownership stakes below the 50 percent threshold;
- Change of ultimate beneficial owner shortly before or after sanctions are imposed;
- Movement of assets previously associated with a sanctioned person, by family members or otherwise on their behalf;
- Numerous transfers of shares from sanctioned entities to non-sanctioned entities involving corporations incorporated by the same individuals or entity (often with a registered office at the same physical address);
- Potential control of an entity by a designated person, despite apparent direct ownership under the 50 percent threshold (member of Board of Directors, beneficial owner, managing director, other entities or persons on the ownership structure linked with a designated person);
- CEO/manager is never available for discussions, i.e., all communications go via a regular employee or a representative who seems to have a general Power of Attorney (PoA).

⁸ This list is indicative and should be supplemented by updated typologies that may have been detected on the basis of information shared by the Commission, the Member States or exchanges with representatives of operators.

Access to EU Commission documents and resources

Commission website (opinions, FAQs)

<https://commission.europa.eu/sanctions>

Consolidated List of Financial Sanctions

<https://webgate.ec.europa.eu/fsd/fsf>

EU Sanctions Map

<https://sanctionsmap.eu>

FAQ on restrictive measures in the area of aviation

<https://www.easa.europa.eu/en/the-agency/faqs/eu-restrictive-measures-against-russia>

EU sanctions whistleblower tool

Sharing of information about EU sanctions violations can contribute to the success of investigations in EU Member States and increase the effectiveness of EU sanctions.

If you are aware of possible violations of any EU sanctions, you can bring this to the Commission's attention in a fully anonymous way. The information can relate, for example, to facts concerning sanctions violations, their circumstances and the individuals, companies and third countries involved. These can be facts that are not publicly known but are known to you and can cover past, ongoing or planned sanctions violations, as well as schemes to circumvent EU sanctions.

https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources/eu-sanctions-whistleblower-tool_en

Contact

If you want to exchange directly with the Commission:

On EU sanctions in general

RELEX-SANCTIONS@ec.europa.eu

On EU sanctions against Russia

EC-RUSSIA-SANCTIONS@ec.europa.eu

As a non-EU stakeholder

EC-SANCTIONS-INTERNATIONAL@ec.europa.eu

National competent authorities for the implementation of EU sanctions

[National competent authorities for the implementation of EU restrictive measures \(sanctions\) \(europa.eu\)](#)

