**Technical Paper**

**Detecting and Preventing Sanctions Evasion and Circumvention in Trade**

**Practical Guidance for Economic Operators**

The EU has imposed unprecedented restrictive measures on Russia that cover approximately 50 percent of the EU trade with Russia. The effectiveness of EU sanctions on trade is eroded and reduced by sanctions evasion and circumvention. Russian and Russia-related EU and third country economic operators have invented numerous ways to evade and circumvent EU sanctions. While the main focus is on individuals and entities that facilitate sanctions evasion intentionally and knowingly, it is equally important to note that facilitation of sanctions evasion may equally happen due to lack of information and adequate training both in the private and public sectors.

Sanctions Regulations are directly applicable law in the European Union Member States. Sanctions circumvention is prohibited by the Regulations and circumvention is punishable criminal activity according to Member States legislation. EU’s sectoral sanctions and individual sanctions against Russia should be implemented in parallel. This means, for example, that if an export operation is not prohibited by the sectoral sanctions, the company should still implement individual sanctions and make sure that the exported goods or technologies do not benefit the sanctioned parties or entities under their ownership or control. The sanctions risk assessment is an obligation of all economic operators. In order to ensure that economic operators make informed business decisions on the best available information concerning sanctions risks, sufficient due diligence procedures, including Know Your Customer (KYC) procedure, shall be ensured and those accordingly thoroughly documented.

This Technical Paper addresses the need for practical guidance to detect and prevent sanctions evasion and circumvention. The Paper presents due diligence recommendations and red-flags for detecting potential sanctions evasion and circumvention by so far identified in co-operation of European authorities. The Paper suggests practical ways to investigate and detect sanctions evasion and circumvention. Any information on possible or detected sanctions evasion or circumvention should be reported to the National Competent Authorities in the EU Member States. This Paper is a living document and will be updated as soon as the need has been identified.

**What is risk assessment and which factors should it take into account?**

A risk assessment (for more information please refer, for example, to [Q&A due diligence on restrictive measures](https://finance.ec.europa.eu/system/files/2020-01/faqs-restrictive-measures-iran_en.pdf)) is a process to identify potential risks by evaluating the probability of the occurrence of an event and the potential damage caused by the event. The scope and extent of the assessment could take into account the following points:



**Purpose of the use**

(military or civilian)

**Other involved parties**

**Target**

(background of customer, business partner, supplier, vendor)

**End user**

(Governmental, military, private)

**Volume of the contract and transactions/payment channel**

**Goods**

**Issues to be considered in the company’s KYC Procedure**

Analysis of possible sanctions evasion or circumvention risks should be part of your usual KYC. The following main questions should be taken into account when performing KYC Procedure:

* Is your product/service subject to sanctions?
* Is your business partner on the sanctions list, or owned or controlled by a sanctioned party?
* Is your business partner connected to entities related to e.g., Russian defense sector or entities suspected or known for trading sanctioned goods and technologies to Russia?
* Is a shareholder, any member of governing body of your business partner (management board, supervisory board or similar) or any C-level employee (e.g., Chief Executive Officer (CEO), Chief Financial Officer) linked to entities related to e.g. Russian high-ranking officials / politically exposed persons (PEPs), Russian defense sector or entities suspected or known for trading sanctioned goods and technologies to Russia?
* What is the planned transaction and is there a risk for circumvention of sanctions? Does the case have any of the characteristics of the red-flag situations (see the detailed list of possible red-flags below)?
* Who is the end user? Can the end user certificate be provided?
* Does your business contract include sanctions circumvention and responsibility clause?
* Have you established your company internal processes for the KYC including documenting the KYC process in a written format?

**Red-flags in Russia or third country related business operations:**

1. European company’s **export is redirected to third countries**, the economic operators of which are known to help Russian economic actors to import sanctioned good and technologies, and there are sufficient grounds to believe that **the final destination of the goods and technologies is Russia**;
2. **New** business partner in a **third country**;
3. Business partner had been **recently established** or has merged with a sanctioned entity or an entity linked to sanctioned entities or persons;
4. Business partner **shares address** with several dozens of different companies (e.g., it is likely a shelf company);
5. 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);
6. **Changes** in ownership **structure** (the company will change ownership to a non-sanctioned entity, especially when the transfer of ownership is linked in time to the sanction status)
7. **Complexity** of ownership or management arrangements and use of **undercover companies** (including the use of family members, complex business arrangements, transfers of shares, change of company names, use of well-known offshore locations);
8. **Location** of Russian companies **in conjunction with sanctioned entities** and participation in trade;
9. Business partner is a company focusing on **freight transport** (transport companies have been used to circumvent sanctions) or agency/mediator/broker of goods or services;
10. Economic indicators:
	1. **Unusual** payment **methods** or currency.
	2. **Multiple** payment **arrangements.**
	3. **Transfers** are **connected to sanctioned** individuals or entities (e.g., payments on behalf of a sanctioned entity.
	4. Payments are made to or come from **third parties**.
	5. **Russian or Belarussian domains** for electronic communications.
	6. **Russian or Belarussian telecoms** operators’ services (identifiable by area code).
	7. Preference to **encrypted messaging platforms** for communications, e.g. whatsapp, signal etc. with **no** apparent **reason**.
11. Other signs e.g. entering into a trade agreement with a **third party**, use of **family members**);
12. **Product and service related**:
	1. Crypto services[[1]](#footnote-1):
		1. A customer’s transactions are initiated from or sent to Internet Protocol (IP) addresses in Russia, Belarus or FATF-identified jurisdictions with AML/CFT deficiencies.
		2. A customer’s transactions are connected to **virtual currency addresses** linked to **sanctioned** subjects.
		3. A transaction has direct or indirect transactional exposure to **virtual currency exchanges** or services located in **Russia**.
		4. A customer initiates a transfer of funds involving **crypto mixing service**.
	2. Account **transfers** (including cross-border credit transfers);
	3. **Cross border** movement of money;
	4. Use of **valuable assets**;
	5. Covering the origin of merchandise:
		1. Product code **alteration**.
13. **Sector related issues**:
	1. Transport sector, logistics – essential for circumventing trade sanctions:
		1. The customer purchasing the goods is **recently registered**.
		2. The activity of the customer **does not correspond** to the category of the purchased product.
		3. The goods are transported by **illogical route** (longer or unusual route).
		4. The customer before 24 February 2022 had business relationships with individuals or entities now **designated** and/or had dealings that involve products that are currently subject to **export restrictions**.
		5. The customer provides **incomplete information** about the end-user and/or end-use of the product, when asked avoids providing additional information.
		6. The description of the goods on the trade/financial documentation is **vague and misleading**.
	2. Legal and tax advisory companies – possible facilitators of circumvention of sanctions, a short distance from legal consultations on compliance with sanctions to assistance in circumvention of sanctions.
	3. Energy sector – transportation companies and transit ports.
	4. Electronic sector and aviation — direct risk for military use in Russia.
	5. Agricultural sector, e.g. cereals.
14. Typical red-flags for money laundering (please see the list on web page www.rahanpesu.fi) – *reference either to local or some international lists.*

**Practical guidance to European companies on due diligence when estimating the risk on sanctions evasion and circumvention:**

1. **Ensure you collect at least the following basic level information from your customer:**
	1. Full name of the entity.
	2. Legal form (listed, limited, private joint stock etc.).
	3. Registration ID.
	4. Private or state-owned.
	5. Key contact, address, phone and homepage URL.
	6. Management full names, date and place of birth, ID Number, PEP status.
	7. Shareholder full names and number of shares, date and place of birth, ID Number, Politically Exposed Person (PEP) status.
	8. Ultimate beneficial owner (UBO, please see Annex I for further information).
	9. Ties of management and shareholders to PEPs and sanctioned subjects.
	10. Activities, products.
2. **Perform open source and sanctions checks.**
	1. **Open-source intelligence**: search company website, news, internet. Media databases and general media should be consulted in order to detect information related to issues such as:
		1. Association with terrorist financing or terrorist activities.
		2. Links to organized crime or arms trafficking.
		3. Money laundering.
		4. Regulatory investigations and material litigation.
		5. Allegations of involvement in bribery and corruption; and/or
		6. Regulatory investigations or sanctions.
	2. **Sanctions check:** Search all company, shareholder and management in the EU Consolidated Financial Sanctions List and other relevant sanctions list (e.g., US SDN List). **Note that sanctions screening for designated entities is an absolute requirement**.
3. **Check whether you really know your business partner and the destination of the goods and technologies by answering the following questions:**
	1. Do you know your current and future business partners (KYC compliance), their background and chains of ownership, and control and management?
	2. Does your customer/business partner operate through the chain on, where it is complicated to track the chain of ownership until the true beneficial owner?
	3. Do you know their business and possible changes in the business profile? Does the partner have connections to PEPs or sanctioned persons or entities, or did have?
	4. In the case of a new business partner, what is the reason for the new business relation?
	5. Does your new business partner have a physical residence and public-facing website?
	6. Is the customer’s line of business in line with ordered/provided goods and technology?
	7. How credible is the final use of the exported goods or technologies in the light of the business profile and company’s projects? Can the company provide enough documentation to prove the final use?
	8. Where have been the products/technology that your business partner provides/sell sourced?
	9. How are the goods/technology in reference transported? What routes are going to be used?
	10. Did your customer/business partner provide written documentation on the company background and the business case?
	11. Does your customer trade in goods/technology that are subject to export/import restrictions?
	12. Is the final end-use of goods/technology that are exported to third countries a logistics warehouse?
4. **Use official sources to verify collected information:**
	1. Official Registers of Companies.
5. **Use your networks to source additional information or share the information (if needed):**
6. Ask for additional information from your EU business associations and MS business associations abroad.
7. Make use of the experience of the other companies on the market (if applicable).
8. **Document background checks and investigation**
9. Document the process:
	1. sanctions screening.
	2. adverse media screening.
	3. communication with the customer/business partner on the case.
	4. inquiries to different parties.
10. Document the information received in the process and the facts that you are basing your business decision on.
11. **Inform the authorities on the sanctions evasion and circumvention cases**
	1. Inform your national competent authority (NCA) on the attempts and detected cases sanctions evasion and circumvention (or the suspected efforts to do that) detected by you (the list of contact points is provided in Annex II to this Technical Paper).
	2. Inform about evasion or circumvention of sanctions by using [EU Whistleblower Tool](https://eusanctions.integrityline.com/setup).

**ANNEX I**

**What is the “ultimate beneficial owner” and why does it matter?**

For an EU operator, it is not always evident who has direct or indirect control over its business partner[[2]](#footnote-2). However, EU operators **must ensure** that they do not make economic resources available (directly or indirectly) to a person or entity who is subject to EU restrictive measures by dealing with an entity, which is controlled or owned by such a person or entity.

**An ultimate beneficial owner** is any natural person who ultimately owns or controls a corporate entity or other legal entity and/or the natural person(s) on whose behalf a transaction or activity is being conducted. As a general rule of thumb (and without prejudice to the specific circumstances of a case), the ultimate beneficial owner of a legal entity may be the natural person who:

* holds an equity interest of at least 25%; or
* wields at least 25% of the voting rights; or
* is the beneficiary of at least 25% of the equity.

Other legal rights may confer control over the EU operator’s business partner to a person or entity who is subject to EU restrictive measures. Such rights may include the possibility to appoint the members of the management or supervisory board, to exercise a dominant influence on legal and business decisions or to act as a major financier. EU operators might consider referring to Article 3(6) of Directive (EU) 2015/849 (Anti-Money Laundering Directive) in order to find further details on identifying beneficial owners for legal persons and legal arrangements.

**ANNEX II**

**Contact points (***of the MS concerned***):**

1. For more red-flags on crypto services refer to: [FinCEN Alert, FIN-2022-Alert001, March 7, 2022](https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%20508.pdf), [Special Bulletin on Russia-linked money laundering activities (canada.ca)](https://fintrac-canafe.canada.ca/intel/bulletins/rlml-eng.pdf) [↑](#footnote-ref-1)
2. [Q&A due diligence on restrictive measures for eu businesses dealing with Iran (europa.eu)](https://finance.ec.europa.eu/system/files/2020-01/faqs-restrictive-measures-iran_en.pdf) [↑](#footnote-ref-2)