



SANCTIONS

SANCTIONS RISK MANAGEMENT POLICY

Compliance

INTRODUCTION

Kernel (hereinafter referred to as the Company, Kernel) is committed to conducting business in accordance with the highest ethical standards.

This includes compliance with all relevant economic and trade sanctions regulations and other restrictive measures in the countries in which we operate and a "zero tolerance" approach to violations of sanctions obligations and requirements by Kernel and its counterparties.

As a Company of integrity, we conduct our business in accordance with the highest ethical standards, complying with all sanctions laws in our operations around the world.

The Sanctions Risk Management Policy (hereinafter referred to as the Policy) has been developed to assist Kernel's employees and counterparties:

- to determine in which processes and at what stages the risks in the area of sanctions regulation may be realized;
- to direct their actions towards making correct and legitimate decisions;
- to ensure a correct understanding of the Company's overall position in the area of sanctions regulation.

I. GENERAL PROVISIONS

Purpose

Ensuring monitoring, assessment, and settlement of sanctions risks in the course of Kernel's business activities.

Objective

Preserving Kernel's business reputation, avoiding cases of cooperation with counterparties subject to international and/or national sanctions, related financial, operational and other sanctions risks, and ensuring the continuity of business processes.

Scope of Application

Kernel is committed to complying with all applicable economic and trade sanctions laws in all jurisdictions in which the Company operates.

This Policy applies to Kernel's operations in all countries and/or jurisdictions, including all subsidiaries and legal entities owned by Kernel, and to all owners, directors, officers, employees, representatives and all business partners of the Company (customers, suppliers, contractors and others), including potential business partners and other third parties acting on behalf of the Company.

Violations of the sanctions laws may result in severe administrative and/or criminal penalties against the Companies and its individual officers, including significant monetary fines, imprisonment, extradition, blacklisting, revocation of licenses and suspension of directors, damage to reputation and commercial relationships, restrictions on the way we conduct business, investigations by government regulators and the imposition of fines or other restrictions by them.

II. PRINCIPLES

- **Compliance with requirements:** following and complying with all sanctions requirements applicable to Kernel's business
- **Preventing violations:** any violations of sanctions requirements by both Kernel and its counterparties
- **Monitoring:** continuous monitoring of sanctions requirements and legislation

III. SANCTIONS RISK MANAGEMENT

Sanctions risks are any possible negative consequences for the Company caused by cooperation with a sanctioned entity, a sanctioned country or an entity that has violated sanctions legislation.

The sanctions risk management process set out in this Policy allows the Company to identify potential areas in which it may directly or indirectly interact with persons, parties, countries or regions prohibited by sanctions and minimize the risks from such interaction.

The presence of sanctions risks is determined by:

- Definition of sanctions risk factors in this Policy;
- Comprehensive due diligence of potential and existing counterparties prior to interaction with them and on a periodic basis;
- Assessment of territorial risks (including the country of origin of goods, registration of the counterparty and its branches and separate subdivisions, place of residence, etc.);
- Assessment of the legality of transactions;
- Implement effective communication and training for employees and counterparties on economic and trade sanctions.

Kernel is committed to managing sanctions restrictions imposed by the United Nations Security Council, the U.S. Treasury's Office of Foreign Assets Control, the U.S. Department of Commerce's Bureau of Industry and Security, the U.S. Department of State, the European Union, Ukraine, the United Kingdom, or any other country or organization whose decisions and acts are legally binding.

IV. COOPERATION WITH COUNTERPARTIES

Kernel is committed to building business relationships with its counterparties on the basis of transparency and integrity.

The Company is open to cooperation with counterparties that share the purpose of this Policy, take measures to avoid sanctions risks in their activities and ensure that neither they nor, to the best of their knowledge, any of their subsidiaries and any official who has the right to sign or makes key decisions in the counterparty's activities, or a representative of any of its subsidiaries or related parties, are:

1. An entity under sanctions;

2. A person who:

(i) is owned or controlled by a Sanctioned Entity; or

(ii) is domiciled, incorporated or resident in a sanctioned country/territory; or

(iii) conducts any business transactions with a Sanctioned Entity; or

(iv) received any funds or any other tangible assets from a Sanctioned Entity; or

(v) carry out any business transactions with an individual or legal entity that is actually located (residing), registered in the sanctioned country/territory, or is a resident thereof;

3. An entity included in the list of entities (the list of residents and persons associated with the aggressor state) that fall under the provisions of the Resolution of the Cabinet of Ministers of Ukraine No. 187 of 03/03/2022 "On Ensuring the Protection of National Interests in Future Claims of the State of Ukraine in Connection with the Military Aggression of the Russian Federation" and the Law of Ukraine On the Basic Principles of Compulsory Seizure of Property of the Russian Federation and its Residents in Ukraine No. 2116-IX of 03/03/2022

V. FACTORS OF SANCTIONS RISKS OF COUNTERPARTIES

When conducting counterparty due diligence, Kernel's authorized employees take into account the following **sanctions risk factors**:

- The counterparty or the counterparty's bank is a Sanctioned Entity, is registered in a Sanctioned Country/Territory, or is controlled or affiliated with a Sanctioned Entity;
- The counterparty or the counterparty's bank is in violation of the sanctions legislation;
- The counterparty is related by ownership or control to the Sanctioned Entity and holds 10% or more of the authorized capital or votes in the executive body and/or ownership structure of the Sanctioned Entity, or is a resident, citizen or permanent resident of the Sanctioned Country (including citizens of the Russian Federation and the Republic of Belarus, except for those who legally reside in the territory of Kernel's business activities);
- Confirmed information was found regarding the counterparty that it uses goods/services originating from sanctioned countries/territories in its business activities;
- The activities of the counterparty are directly or indirectly influenced by the Sanctioned Entity (in particular, through indirect ownership or voting rights);
- There is information confirming that the UBO/recipient/consumer/producer/consignor/carrier/consignee is a Sanctioned Entity;
- An agreement concluded with a counterparty signed by a Sanctioned Entity;
- Whether the counterparty has representative offices and/or offices in the country/territory under sanctions, as well as suppliers, buyers, subcontractors, carriers, manufacturers, consignees, and other partners registered and/or located in such territories that are involved in the performance of the contract with Kernel or in the payment route under this contract;
- The counterparty refuses to sign the Kernel model anti-corruption/sanctions clause in full or in part as part of the transaction;
- Other factors defined by the current legislation of Ukraine.

VI. MANAGING THE RISKS OF COOPERATION WITH THE AGGRESSOR STATE

Pursuant to the requirements of the current legislation of Ukraine, in carrying out its activities, Kernel takes the following measures to prevent cooperation with counterparties associated with the aggressor states that are considered to be aggressors:

- Citizens of the Russian Federation, except for those legally residing in Ukraine;
- Legal entities registered in accordance with the laws of the Russian Federation;
- Legal entities established in accordance with the laws of Ukraine, UBO, a shareholder with a share in the authorized capital of 10% or more is a citizen of the Russian Federation, except for those who legally reside in Ukraine.

Kernel undertakes to refrain from performing any actions and conducting any business activities with counterparties associated with the aggressor state, including but not limited to the following:

- Fulfilment of any obligations to the aggressor state or persons related to it;
- Alienation, lien, or any other actions that have or may result in the transfer of property to the aggressor state or a person related to it.

In order to manage the risks of cooperation with the aggressor state, all contracts with Kernel's counterparties include an [anti-corruption/sanctions clause](#).

If you refuse to sign such a clause in full or in part, the risk of cooperation with the counterparty automatically increases.

Kernel takes all necessary measures to prevent cooperation with counterparties whose activities have signs of collaboration.

VII. AREAS OF RESPONSIBILITY

Employee/Initiator:

- Initiating a counterparty due diligence prior to entering into a contract;
- Gathering preliminary information about the counterparty;
- Reconciliation of identified risks;
- Implementing the recommendations of the Compliance Department to minimize/eliminate sanctions and any other risks.

Security Department:

- Due diligence of counterparties and provision of conclusions based on its results;
- Periodic updating of inspections to identify cooperation risks in a timely manner;
- Maintaining the IAS "Security Management System";
- Requesting the Head of the Compliance Department to assess sanctions and other compliance risks.

Head of the Compliance Department:

- Assessment of the situation, provision of a conclusion on the level of compliance risk and recommendations for its minimization/elimination.

Head of the initiator:

- Deciding on the possibility of cooperation with counterparties in respect of which risks of the appropriate level have been identified.

Tender commission (if necessary):

- Deciding on the possibility of cooperation with counterparties in respect of which risks of the appropriate level have been identified.

Managers/Tender Commission:

- Making a decision on cooperation if a "high" level of cooperation risk is identified;
- Submitting the issue of further cooperation with the counterparty for consideration by the Risk Committee in case of a "high" compliance risk.

Risk Committee:

- Deciding on the possibility of cooperation with the counterparties identified as having a "high" sanctions or other compliance risk.

VIII. FINAL PROVISIONS

VIII. OTHER PROVISIONS

▪ **Approval and revision of the Policy**

This Policy shall be approved by the General Director and shall come into force upon its approval.

Changes and additions to this Policy may be initiated by employees of the Compliance Department, Security Department and Legal Department.

In case of urgent changes, the Head of the Compliance Department initiates its update within 30 working days from the date of receipt of such proposals.

- Each Employee of the Company, including temporary ones, shall be personally liable to the management and owners of the Company in case of violation of the requirements of this Policy and actions that will lead to reputational risks for the Company.
- Each employee of the Company is obliged to report violations through the Hotline 0 800 501 483 or by e-mail hotline@kernel.lu or contact the Compliance Department compliance@kernel.lu

Process owner: Head of the Compliance Department

Developed by: Head of the Compliance Department

Related documents:

- Corporate Code
- Code of Interaction with Suppliers
- Procedure "Receiving and reviewing information received through the Hotline channels"
- Procedure "Conducting corporate investigations"
- Procedure "Protection of Applicants"
- Procedure "Verification of Counterparties by the Security Department"
- Procedure "Creation and approval of economic and legal documents"

XI. UNACCEPTABLE ACTIONS

- Interact with counterparties without preliminary verification
- Interact in any way with the aggressor state
- Non-compliance with the requirements and principles of this Policy
- Any actions that may result in financial or reputational losses for the Company

TERMS AND DEFINITIONS

Sanctions are special economic and other restrictive measures that can be applied to protect national interests, national security, sovereignty and territorial integrity of a country, counter terrorist activities, as well as prevent violations, restore violated rights, freedoms and legitimate interests of citizens of any country, society and state. Sanctions may be imposed on certain countries, individuals or legal entities (groups of individuals), types of economic activity and/or types of goods (services), and the territory of origin of goods (services).

International sanctions are restrictions imposed by the UN Security Council, the U.S. Treasury Department's Office of Foreign Assets Control, the U.S. Department of Commerce's Bureau of Industry and Security, the U.S. State Department, the European Union, Ukraine, the United Kingdom, or any other country or organization whose decisions and acts are legally binding.

National sanctions are restrictions applied to protect the national interests and national security of Ukraine.

Prohibited Territory means any country subject to any sanctions rules adopted or applied by any sanctions authority, including the Russian Federation, the Republic of Belarus, Iran, Syria, Cuba, North Korea, Sudan, the Autonomous Republic of Crimea and the city of Sevastopol, the temporarily occupied territories of Ukraine, other countries or territories subject to sanctions.

TERMS AND DEFINITIONS

Sanctioned entity is a legal entity regardless of ownership, a group of companies, a foreign legal entity, a legal entity controlled by a foreign legal entity or a non-resident individual, an individual, a foreigner, a stateless person, an aircraft, a ship or other vehicle that is subject to international and/or national sanctions. If a country is a sanctioned entity, all legal entities and individuals within that country, namely (a) in the case of legal entities, those that are registered, actually located in such country and/or the beneficial owners or other persons exercising control over such legal entity are citizens, residents of such country, actually residing in such country or otherwise connected with the sanctioned country; (b) with respect to individuals, those who are registered, residing, domiciled in, or otherwise associated with a sanctioned country are treated as a sanctioned entity.

Collaborative activities are actions aimed at benefiting a state that has committed armed aggression against Ukraine.

Ultimate beneficial owner (hereinafter referred to as the UBO) is any individual who exercises decisive influence (control) over the activities of a legal entity in accordance with the Law of Ukraine On Prevention and Counteraction to Legalization (Laundering) of Proceeds of Crime, Terrorist Financing and Financing of the Proliferation of Weapons of Mass Destruction No. 361-IX of 06/12/2019.

Aggressor state is a state that has occupied a part of the territory of Ukraine in any way or is carrying out any aggression against Ukraine.