Protecting investments: accurate legal compliance with sanctions, anti-money laundering and anti-corruption

PIETRO FANTAPPIÈ
Senior Associate, LegaLife Diaz Reus

Pietro is an international lawyer with several years of experience who focuses his practice on the retail sector and service industries such as real estate and hospitality, cross-border transactions, blockchain and ICO, fraud, and commercial law.
He also assists high net worth clients with international planning. Pietro holds a diploma in Business Administration from London's Westminster College and a J.D. equivalent from the University of Florence, Italy.

ANNA SHASHKOVA
Of Counsel, LegaLife Diaz Reus

Anna has been practicing law for more than 19 years.
Her practice includes in-depth expertise on money laundering and fraud, constitutional law, as well as corporate, business, and tax law.
She is also a law professor at Moscow State Institute of International Relations (MGIMO), has widely published books on money laundering, Russian business law, and Russian corporate and business law, and authored over 150 publications in periodicals such as "Lawyer," "President Control," "Rossiyskaya Ustitsya," etc.
She graduated with distinction from MGIMO and obtained a Ph.D. in Law from MGIMO.

What is compliance?

Compliance means an act of obeying an order, rule, or request. In worldwide practice, compliance departments are created both to identify and minimise the risks that organisations face and to resolve compliance difficulties when they occur. In the Russian Federation such a term does not have an official legislative interpretation though quite a large number of Russia-based companies have established their own internal Compliance Departments.

Companies should adopt and implement a corporate governance compliance programme (CGCP) that includes, among others, specific compliance with sanctions and anti-money laundering (AML) and corruption laws and regulations. With CGCP we define compliance obligations associated with certain critical aspects of corporate governance in the current global geopolitical and business environment, namely with being a good corporate citizen in Russia and in international business, especially in the financial community. It is recommended that all major Russian companies, as well as international entities operating in Russia, learn and adopt a culture of compliance under the heading of CGCP for the reasons explained below and continuously review their compliance.

Why complying?

Strict legal compliance with AML and corruption legislation is required. Notwithstanding the absence of criminal liability of corporations in Russia, penalties under the Code for Administrative Violations of the Russian Federation may be imposed, such as high mon-

etary fines and disqualification of top employees. Directors, owners, and top executives of businesses may also face criminal liability, which can include fines, disqualification of up to 5 years, or imprisonment of up to 7 years. From an outside point of view, any AML or corruption non-compliance may also result in criminal liability that can be even more severe than in Russia, as well as result in sanctions against a particular company or particular individual by US and European Union authorities, which may result in huge financial losses.

Compliance with sanctions

More so than ever before, companies operating in Russia must develop and implement Office of Foreign Assets Control (OFAC) sanctions detection and monitoring programmes. Sanctions are instruments intended to create a negative atmosphere as well as business and personal consequences when it comes to investments and the way people do business in general. Specifically, sanctions aim to freeze financial assets which belong to legal entities and individuals, often affecting at least one of the most personal spheres of freedom – property. Sanctions may be considered as administrative measures with no apparent remedy and are often enacted based on political motives. It can be argued that sanctions are always political in nature, since they are enacted by executive branches (governments) of countries.

In the present context of sanctions against the Russian Federation and other jurisdictions, there is a real element of risk when investing in business activities in Russia that do not comply carefully with the international sanctions' regime, namely engaging in prohibited financial and transactional operations, investments, trading, or other activities, especially with sanctioned persons and entities.

Thus, sanctions do not only carry a psychological impact when hindering potential investors from new activities, but they cause very real risks and negative consequences for those who engage in business with sanctioned entities without assessing and implementing proper conduct. It is therefore necessary to carefully consider precautionary measures in order to set up appropriate sanctions compliance activity and thus create ideal conditions for risk-free transactions that are reliable for investors. Such an approach is rather important nowadays in the context of international business investments, and business in the Russian jurisdiction is no exception.

Sanctions cause very real risks and negative consequences for those who engage in business with sanctioned entities without assessing and implementing proper conduct.

In order to have a better understanding of the issue of sanctions from a legal perspective, it is very important to identify some of the major players and their powers to enact and implement such measures – OFAC and the European Council.

OFAC, which acts under the US Department of Treasury (executive branch), is the relevant office that publishes and continually updates a list of Specially Designated Nationals and Blocked Persons (*"SDN List"*), as well as a list of Specially Designated Narcotics Traffickers (*"SDNT List"*). Sanctioned person(s) and/or entities placed on the SDN or SDNT Lists, including those placed on the SDN List pursuant to GLOMAG (2016 Global Magnitsky Human Rights Accountability Act), may have their US-based property and interests in property "blocked". Businesses and investors must be aware that their failure to comply with OFAC sanctions *will lead to the "blocking" of wire transfer payments, the loss of international banking privileges, and potential civil and criminal penalties.* There are many other direct consequences and collateral consequences, among others being stopped for secondary inspection and denied entry at immigration and customs entry points into the US, and being placed on US airlines' "no-fly" lists. Sanctions compliance can, however, be put in place by companies by studying their business relationships in order to identify potential risks of OFAC sanctions and their consequences. An appropriate OFAC compliance programme should be implemented to avoid these costly repercussions. It must be stressed that even if an individual or entity is placed on OFAC's SDN list, it is still possible to act legally and seek *"de-listing"*. De-listing from the SDN or SDNT Lists, including those placed on the SDN List pursuant to GLOMAG, regularly occurs by filing a timely request for reconsid-

eration. There are two ways to appeal OFAC's denial of a reconsideration request: (1) submitting a new administrative reconsideration; (2) initiating a lawsuit under the Administrative Procedure Act ("APA") against OFAC in the US District Court of Appeals for the District of Columbia.

OFAC administers a number of different sanctions programmes not related to a particular jurisdiction. *Thus, it is vital to stress that proper business conduct is not limited to behavior in one jurisdiction, but applies to relations with sanctioned entities and business activities in any other jurisdiction,* as the recent case of Russia's Agrosoyuz Commercial Bank demonstrates. On August 3, the Treasury Department imposed SDN sanctions on Agrosoyuz Commercial Bank over handling transactions for North Korea in violation of United Nations restrictions.

In the EU, sanctions against other jurisdictions are usually enacted after a vote by the European council, which involves all the heads of states and governments of the 27 member states.

Anti-money laundering compliance

All companies, especially financial institutions, should develop and implement "gold standard" AML in accordance with the internal laws of the company's jurisdiction as well as relevant international treaties and agreements. Effective AML requires the following: (1) written policies and procedure; (2) compliance; (3) training; and (4) audit. Such a comprehensive AML programme will help companies preserve their important banking relationships and avoid law enforcement scrutiny and investigation which, in case of non-compliance offenses, can result in jail sentences, high monetary fines, and other penalties.

The main relevant act of the Russian Federation to comply with in this field is the Anti-Money Laundering Law (*Federal Law No. 115-FZ on Countering Legalisation [Laundering] of Proceeds from Crime and Financing of Terrorism*) dated August 7, 2001, which is regularly amended (last amendments came into force on July 23, 2018).

There are also plenty of other regulatory acts issued by AML regulators.

The general authority is the Federal Financial Monitoring Service (*Rosfinmonitoring*). It requires individuals trading commodities or on financial markets to provide information upon request, gathers and analyses reports of suspicious transactions, prosecutes violations of AML legislation, and transfers the collected data to the appropriate law enforcement authorities for further investigation and action. Multiple orders of Rosfinmonitoring shall be complied with.

Among other domestic AML regulators are the Government of the Russian Federation, the Bank of Russia, the Ministry of Finance, the Assay Chamber (under the supervision of the Ministry of Finance), the Federal Supervision Service for Communications, Information Technologies and Mass Communications (*Roskomnadzor*), and the Federal Tax Service, which issue various resolutions and orders to comply with. Each of these state bodies have their own specialisation, e.g. the Bank of Russia is responsible for credit organisations, insurance companies, and professional participants in the securities market, while the Assay Chamber is in charge of entities engaged in trade in precious metals, gemstones, and jewelry. In the last 4 years, the Bank of Russia has revoked more than 350 bank licenses (96 in 2016, 51 in 2017, 28 during the first half of 2018) for non-compliance with AML requirements and other violations. Internationally there are many relevant bodies as well.

Corruption compliance

There is much more emphasis throughout the global business community on suppressing all forms of corruption. Global and Russian companies must develop a general awareness of the perils of paying kickbacks or bribes, and must learn how to avoid dealings with corrupt officials, including with corrupt foreign officials or Politically Exposed Persons (PEPs).

Companies must be aware of the Foreign Corrupt Practices Act, a US federal statute that prohibits US companies, or other companies under US jurisdiction (any foreign company, including a Russian one, can under certain circumstances fall under US jurisdiction), from bribing public officials to obtain a commercial advantage. The US Department of Justice has prioritised FCPA investigations and prosecutions to attack this form of business corruption. Global companies must be made aware of FCPA requirements and must train their employees and senior management accordingly. Companies also must be aware of the Magnitsky Act, which authorises and requires OFAC to list and sanction individuals or entities that are involved in corruption or human rights violations.

The Russian Federation is categorised by the US State Department as a jurisdiction of primary concern with respect to money laundering and financial crimes such as corruption. Official corruption remains a problem at all levels of government and a major source of laundered funds, especially in the judicial system and public procurement. The situation with state corruption is considered one of Russia's vulnerabilities. Thus, measures to counter corruption mostly concern government employees, though B2B corruption is also punishable.

Federal Law No. 273-FZ on Countering Corruption dated December 25, 2008 is the main document to comply with in this field in Russia. Many subsidiary documents were later adopted which mainly place additional requirements on government employees. For example, in 2016 state officials were banned from owning securities or other financial assets located or registered abroad through third parties. Russian law controls both income and expenses of state employees. Since 2018 both state and municipal officials may be dismissed on the grounds of loss of trust. Russian law criminalises active and passive bribery, facilitation payments, gifts, and other material benefits.

The President of the Russian Federation adopted 6 National Plans on Countering Corruption, the most recent one on June 29, 2018 for 2018-2020. Other regulatory bodies in the area are the Government of Russia and the Ministry of Internal Affairs of the Russian Federation.

Introduction of compliance practice with corruption norms has been a programme of the fourth step (started in 2010) of combating AML and corruption at the international level and at the level of particular countries. All companies must understand these significant risks of being involved in corruption schemes and must implement the appropriate anti-corruption policies and procedures. If companies fail to address these issues, they may find themselves under criminal investigation for commercial bribery, sanctions violations, or money laundering, and they will suffer significant reputational harm and financial losses.