BORD TA' SORVELJANZA DWAR IS-SANZJONIJIET
SANCTIONS MONITORING BOARD
MALTA

Implementing Article 32

Sanctions Compliance Requirements

Issued by the Sanctions Monitoring Board in terms of the National Interest (Enabling Powers) Act
- Chapter 653 of the Laws of Malta -

First Issued in August 2026

Table of Contents

SMB BORD TA' SORVELJANZA DWAR IS-SANZJONIJIET
SANCTIONS MONITORING BOARD
MALTA

Chapter 1

Introduction and Scope

1.Introduction and Scope

1.1 Background

The National Interest (Enabling Powers) Act ("NIA"), Chapter 653 of the Laws of Malta, establishes a comprehensive legal framework for the implementation of restrictive measures in Malta, giving effect to United Nations ("UN") Security Council Resolutions and European Union ("EU") restrictive measures and making them directly applicable and legally binding in Malta upon adoption.

The NIA empowers the Sanctions Monitoring Board ("SMB") to issue binding guidance and procedures on sanctions implementation, interpretation and due diligence. Pursuant to Article 15(5)(c) of the NIA, these procedures are legally enforceable.

This document (the "Guidance Note") provides practical guidance on the establishment of internal procedures, policies and controls necessary for compliance with restrictive measures in accordance with Article 32 of the NIA as intended for the persons, entities or bodies listed in Schedule I ("Operators")-, setting out the expectations of the SMB.

The term "should" is used throughout this guidance to indicate the expected minimum requirements for operators. Where an operator chooses not to follow this guidance, this may be taken into account as an aggravating factor in any enforcement action if the operator is found to have breached the sanctions regime.

Operators should use this Guidance Note to inform the development and implementation of their internal Sanctions Framework, ensuring that internal policies, procedures and practices are fully aligned with the expectations set out in this document. Controls should be properly documented, maintained, and open to verification. Operators should also be aware that failure to implement appropriate controls may be used as evidence in criminal proceedings.

1.2 Sanctions and Managing Sanctions Risk

Sanctions are restrictive measures imposed to pursue specific foreign policy or national security objectives. In the Maltese legal framework, sanctions may arise from measures adopted by the UN Security Council and EU, which are implemented (in the case of measures adopted by the UN Security Council) or directly applicable (in the case of EU sanctions) in Malta, as well as from national measures adopted by the Government of Malta.

A breach of sanctions constitutes a criminal offence and may result in a fine and/or imprisonment. It may also expose Operators to legal, regulatory, and reputational consequences.

Natural or legal persons, entities or bodies subject to sanctions are referred to as "designated persons".

Sanctions measures may take several forms, including but not limited to:

- Financial sanctions, including asset freezes - Financial sanctions restrict access to funds and economic resources belonging to, held by, or controlled by designated persons. This may include asset freezes, which prohibit dealing with such funds or making funds or economic resources available to designated persons.

- Trade sanctions, including arms embargoes and other trade restrictions - Trade sanctions restrict or prohibit the import, export, sale, supply, or transfer of certain goods, technologies, or services to or from specific countries, entities, or individuals. These may include arms embargoes or restrictions on particular categories of goods.

- Immigration sanctions - Immigration sanctions prohibit designated persons from entering, transiting through, or remaining in a country.

- Transport sanctions, including measures relating to aircraft and shipping - Transport sanctions restrict the movement or operation of certain aircraft or vessels, for example by prohibiting them from entering ports or airspace, or by restricting the provision of related services.

Challenges in sanctions compliance

Compliance with sanctions regimes presents practical challenges. Designated persons may seek to conceal or misrepresent their identity in order to circumvent restrictive measures, including by operating through complex ownership structures, using intermediaries, or exercising control over entities in an indirect or informal manner.

In addition, sanctions measures may apply in different ways depending on the circumstances. For example, restrictions may arise where a designated person owns or controls an entity, where funds or economic resources are made available to them directly or indirectly, or where goods or services are provided in breach of trade or transport restrictions. Identifying these risks requires Operators to look beyond their immediate contractual counterparty and consider the broader context of relationships and transactions.

Identifying sanctions exposure beyond the client

A common shortcoming in sanctions compliance is to treat sanctions risk as arising only from the immediate client.

Because designated persons may seek to conceal their identity, it is generally not sufficient for Operators to rely solely on the identity information provided by a client without undertaking further checks.

Sanctions exposure may arise not only through the client itself, but also through persons who own or control that client, whether directly or indirectly. In practice, designated persons may distance themselves from an entity through layered ownership structures, the use of intermediaries, or the exercise of influence or control outside the formal ownership structure.

Risk may also arise through other parties connected to a relationship or transaction, including counterparties, beneficial owners, directors, or third parties providing funding or receiving funds.

For this reason, identifying sanctions risk requires Operators to look beyond the immediate contractual counterparty and consider the broader context of the relationship or transaction.

1.3 Who Needs to Comply with the Law?

The Act applies to any natural or legal person, entity or body, including vessels, aircraft, and other means of transport, that is in, registered in, transits through, or travels to or from Malta. For citizens of Malta, the law applies wherever they are located.

In general terms, to comply with the sanctions regime applicable in Malta, every legal person, entity or body must, inter alia:

- Ensure that they do not make funds or economic resources available to a designated person unless authorised to do so under a licence (this obligation arises under Article 9 (a) of the NIA);

- Prevent breaches of, or attempts to circumvent, restrictive measures-

- Ensure that no conduct is undertaken that would constitute an offence under Article 9 of the NIA and that, pursuant to Article 10 thereof, no action is taken to incite, aid, or abet any commission of such offences. See Annex I for more information.

1.4 Who Needs to Comply to Article 32 in particular?

The obligations under Article 32 of the NIA apply to all Operators listed under Schedule I.

At present, Schedule I largely reflects the categories of “subject persons” defined under the Prevention of Money Laundering and Funding of Terrorism Regulations (“PMLFTR”). As a result, many entities already subject to anti-money laundering and counter-terrorist financing (“AML/CFT”) obligations are also required to comply with Article 32 of the NIA.

The NIA, however, allows the Minister to amend Schedule I from time to time. This means that Article 32 of the NIA may be extended to other operators whose activities present sanctions-related risks, even where those operators are not currently subject persons under the PMLFTR.

Within Operators that fall within Schedule I, responsibility for compliance with Article 32 extends across relevant functions and staff involved in client onboarding, transactions, operations and compliance oversight.

Branches and subsidiaries in third countries

Operators that have branches or majority-owned subsidiaries established in third countries should ensure that those branches and subsidiaries implement the provisions of this Act to the extent that the laws of the relevant third country permit.

Where the legislation of a third country does not permit the implementation of restrictive measures in full, Operators should ensure that appropriate additional measures are applied to manage and mitigate the risk of breaches or circumvention of restrictive measures effectively.
Such measures may include, for example, enhanced oversight from the parent entity, restrictions on certain business activities, additional controls over transactions, or other risk-mitigating arrangements proportionate to the nature and extent of the constraints imposed by local law.

Operators should also ensure that any limitations arising from third-country legislation, and the measures adopted to address them, are appropriately documented and capable of being demonstrated to the SMB upon request.

1.5 Overview of Article 32 Obligations – The Sanctions Framework

Article 32 of the NIA establishes a number of core obligations intended to ensure that Operators can identify and prevent breaches or circumvention of restrictive measures. In practical terms, compliance with Article 32 of the NIA requires Operators to implement a framework of controls (the “Sanctions Framework”) to:

- Assess their exposure to sanctions risks (see Section 3 for additional information);
- Identify their clients and, where relevant, understand the ownership and control structure of legal entities or arrangements (See Section 4 for additional information);
- Screen relevant persons and entities against applicable sanctions lists (See Section 4 for additional information);
- Monitor business relationships and transactions to identify potential sanctions breaches or circumvention risks (see Section See Section 4 for additional information);

- Freeze funds and economic resources where required by applicable restrictive measures (see Section 5 for additional information);

- Report sanctions hits and suspected breaches to the SMB without delay (see Section 5 for additional information);

- Prevent the advance disclosure to clients or third parties that a freezing order is to be applied (see Section 6 for additional information);

- Maintain internal policies and procedures documenting the controls above (see Section 7 for additional information);

- Maintain adequate records demonstrating compliance with these obligations (see Section 8 for additional information); and

- Ensure that any reliance on third parties or outsourcing arrangements does not impair the Operator's ability to comply with its obligations under the NIA and that appropriate oversight is maintained (see Section 9 for additional information);

- Ensure that relevant personnel possess adequate knowledge of sanctions obligations and receive appropriate training (see Section 10 for additional information);

- Ensure that the systems on which their compliance with sanctions obligations relies are adequate (see Section 10 for additional information); and

- Establish governance arrangements that ensure oversight of sanctions compliance within the organisation (see Section 12 for additional information).

Collectively, these measures should be capable of enabling Operators to identify and prevent situations in which funds or economic resources may be made available, directly or indirectly, to designated persons or entities.

Subsequent sections of this Guidance Note set out further guidance on how Operators should implement each component of the Sanctions Framework.

Integration of the Sanctions Framework

For a Sanctions Framework to operate effectively, its various components should not be treated as separate or isolated processes. Instead, they should operate as part of a coherent and continuous system in which each element informs and supports the others.

The different components of the framework such as risk assessment, due diligence, screening, monitoring, and escalation arrangements should be designed to operate as a continuum. The outputs of one component should inform the operation of the others, creating a feedback loop that allows Operators to refine their understanding of sanctions risk and adjust their controls where necessary.

For example, insights obtained through screening, transaction monitoring, or investigations may reveal patterns or vulnerabilities that should be reflected in the Operator's risk assessment and control framework. Similarly, the results of the risk assessment should guide how controls are designed, prioritised, and applied in practice.

Operators should also ensure that the framework is actively used as a decision-making tool. The information generated through the various components of the framework should inform operational and compliance decisions, including how risks are assessed, how controls are calibrated, and how potentially higher-risk relationships or transactions are managed.

In practical terms, this requires the implementation of a framework of controls that begins with an assessment of sanctions risk and extends to the performance of appropriate due diligence on clients and other parties involved in relationship or transaction, the screening of such parties against sanctions lists, and the ongoing monitoring of transactions and business relationships.

Recalling the principle set out pursuant to Article 11(5), where an offence under the Act is committed by a legal person, responsibility may extend to all members of senior management and to any other person exercising control over the operator. Such persons are expected to ensure that effective internal controls and compliance measures are in place and operational, and that a culture of compliance is embedded throughout the organisation. Liability may arise unless it can be demonstrated that the offence was committed without their knowledge and that all appropriate due diligence was exercised to prevent its commission.

1.6 How to Use This Guidance Note

This Guidance Note is intended to assist Schedule I Operators in understanding and implementing their obligations under Article 32 of the NIA in relation to sanctions compliance. In particular, it describes the types of controls, organisational arrangements, and procedures that Operators are expected to have in place in order to identify, assess, and manage sanctions risk and ensure compliance with applicable restrictive measures.

Moreover, this document is intended to apply across the full range of Schedule I operators in all their diversity. This includes sole practitioners as well as large corporations, operators with international exposure as well as those operating solely domestically, operators conducting isolated transactions as well as those handling high transaction volumes, and operators relying on either manual or automated systems.

For this reason, the document establishes minimum requirements rather than highly sector-specific operational examples. We recognise that the practical realities of implementation can differ significantly between sectors. Accordingly, sector-specific guidance will later be addressed through separate guidance documents tailored to specific sectors.

The guidance is legally binding and has effect in law. It supplements and gives practical effect to the relevant provisions of the NIA by setting out the regulator's expectations as to compliance. Accordingly, it clarifies, specifies and reinforces the legal obligations established under the NIA.

What this means is that the term "should" reflects the minimum requirements that Schedule I operators are expected to implement. By contrast, the term "may" refers to optional additional measures that operators can consider adopting to strengthen their controls. Failure to implement requirements expressed through the term "should" may give rise to administrative penalties under Article 35 for breaches of the obligations set out in Article 32.

The examples provided throughout this Guidance Note are intended for illustrative purposes only. They are not exhaustive and are included to assist Operators in understanding how the principles described in this document may apply in practice. Operators should exercise appropriate judgement when applying these principles to their own circumstances and should not rely solely on the examples provided when determining their sanctions compliance obligations.

1.7 Staying Informed

Operators are expected to remain informed of developments in applicable sanctions regimes, including changes to UN Security Council Resolutions and EU and domestic restrictive measures. Operators should therefore ensure that they have mechanisms in place to monitor relevant updates issued by competent authorities and international bodies, including updates directly published in the Official Journal of the European Union.

To support this, operators are encouraged to subscribe to the SMB newsletter and regularly to consult official sources of sanctions information in order to ensure that all components of their Sanctions Frameworks remain up to date.

SMB BORD TA' SORVELJANZA DWAR IS-SANZJONIJIET
SANCTIONS MONITORING BOARD
MALTA

Chapter 2

Foreword on the Interaction between Sanctions Controls and AML/CFT Frameworks

2. Foreword on the Interaction between Sanctions Controls and AML/CFT Frameworks

In practice, many of the controls used to manage sanctions risks overlap with those applied in the context of AML/CFT frameworks. Operators will therefore often rely on the same operational processes, such as customer due diligence, beneficial ownership identification, screening and transaction monitoring, to address both sanctions and AML/CFT risks.

While these frameworks share certain processes and tools, they serve, however, different legal objectives and are subject to distinct regulatory requirements. AML/CFT controls are primarily designed to identify and mitigate risks of money laundering, terrorist financing and related financial crime. By contrast, sanctions controls are intended to ensure that Operators do not make funds or economic resources available, directly or indirectly, to persons, entities, vessels or jurisdictions subject to restrictive measures, and to identify and mitigate risks related to sanctions breaches, sanction circumvention and proliferation financing.

Operators should therefore take care to integrate sanctions controls within their broader AML/CFT compliance frameworks while ensuring that the specific legal requirements and objectives of sanctions regimes are fully met. The two frameworks are closely interconnected, particularly since the intentional violation or circumvention of sanctions constitutes a predicate offence to money laundering. Nevertheless, sanctions compliance obligations extend beyond targeted financial sanctions and encompass all types of sanctions, as well as measures aimed at mitigating proliferation financing risks.

A practical example of this interaction arises in the identification of beneficial owners. Under AML/CFT rules, Operators are generally required to identify natural persons who hold 25 percent or more of the ownership interests in a legal entity. This threshold assists in identifying individuals who may ultimately control or benefit from the entity.

Sanctions regimes, however, apply a different test when determining whether an entity itself becomes subject to restrictive measures. In particular, under EU sanctions practice an entity may be treated as sanctioned where one or more designated persons collectively own 50 percent or more of the proprietary rights in that entity, or where a designated person otherwise exercises control over it.

In practice, Operators can leverage the information obtained through AML/CFT beneficial ownership identification to support sanctions compliance. For example, identifying beneficial owners above the 25 percent threshold provides a useful starting point for determining whether designated persons may hold ownership interests in the entity. However, Operators should remain mindful that sanctions exposure may arise even where a designated person holds less than 25 percent ownership if multiple designated persons collectively exceed the relevant ownership threshold or if control is exercised through other means.

Moreover, sanctions ownership assessments are not limited to natural persons. Unlike AML/CFT beneficial ownership requirements, which focus primarily on identifying natural persons who ultimately own or control a customer, sanctions ownership assessments also require consideration of legal persons within the ownership structure. As such, legal persons holding 50 percent or more of the shares or ownership rights in an entity should be identified and screened as part of the sanctions ownership assessment.

Another practical example concerns high-risk jurisdictions. The scope of sanctions-related risk extends beyond jurisdictions identified as high risk for ML/FT purposes and includes jurisdictions that facilitate, directly or indirectly, the circumvention of sanctions imposed on other countries. These risk exposures are often driven by geopolitical developments and may change rapidly over time.

Operators should therefore design their compliance frameworks in a way that allows AML/CFT and sanctions controls to operate in an integrated manner, while still ensuring that the distinct requirements of each regime are addressed. This approach helps avoid unnecessary duplication of processes while ensuring that both AML/CFT obligations and sanctions obligations are fulfilled effectively and the legal tests required under each regulatory regime are applied.

SMB BORD TA' SORVELJANZA DWAR IS-SANZJONIJIET
SANCTIONS MONITORING BOARD
MALTA

Chapter 3

Sanctions Risk Assessment

3. Sanctions Risk Assessment (SRA)

The starting point of an effective Sanctions Framework is a clear and detailed understanding of the sanctions risks to which an Operator is exposed. This is achieved through the performance of a Sanctions Risk Assessment ("SRA").

Articles 32(5), (6), and (7) of the NIA require Operators to carry out an enterprise-wide SRA. All relevant activity lines of the Operator should be considered within a single entity-level assessment.

The purpose of the SRA is to ensure that Operators understand how their business model, client base, products and services, and transactions may give rise to sanctions risk.

A well-designed risk assessment enables Operators to identify where sanctions risks may arise within their activities, assess the level of risk associated with those exposures, and design and implement controls that are proportionate to those risks.

Important: The scope and depth of the SRA should be proportionate to the nature, size and complexity of the operator's activities. Operators with international operations, cross-border exposure or complex business models will generally face greater sanctions risks and may therefore require a more detailed assessment

A compliant SRA is not optional. It is a statutory duty forming an integral part of an Operator's Sanctions Framework. The effectiveness of a Sanctions Framework ultimately depends on how seriously an Operator treats its SRA. By approaching the SRA with rigour and transparency, and by treating it not as a procedural formality, but as a living tool that informs decision-making, Operators demonstrate not only regulatory compliance but also a genuine commitment to ethical practice and resilience in an increasingly complex global landscape.

3.1 Risk Appetite Statement

In order to operate effectively, an SRA should be conducted with reference to a clearly defined sanctions risk appetite. A risk appetite statement describes the levels and types of sanctions risk that an Operator is prepared to accept in the course of its activities.

The risk appetite statement provides the framework within which sanctions risks identified through the SRA are assessed and managed. It enables Operators to determine whether particular clients, transactions, jurisdictions or business activities fall within the level of risk the organisation is willing to accept. A sanctions risk appetite statement should therefore guide decisions relating to:

- The categories of clients or counterparties with which the Operator is prepared to engage;
- The jurisdictions in which the Operator is willing to operate;
- The products and services that may give rise to sanctions exposure; and
- The level of due diligence, monitoring and control measures required in higher-risk situations.

Operators should ensure that their sanctions risk appetite is documented, approved at an appropriate level of senior management and communicated internally so that relevant staff understand how sanctions risks should be managed in practice.

Operators should also establish arrangements to assess, on a periodic basis, their actual level of sanctions risk exposure. Where this assessment indicates that risks exceed the Operator's defined risk appetite, appropriate action should be taken. This may include the introduction of additional controls, restrictions on certain activities or, where necessary, the termination of business relationships that fall outside the Operator's risk tolerance.

The sanctions risk appetite statement may be maintained either as a standalone document or as part of the sanctions risk assessment itself, provided that it remains properly documented, up to date, and readily available upon request.

Where the sanctions risk appetite statement is maintained separately from the sanctions risk assessment, it should be provided together with the sanctions risk assessment upon request by the SMB or the relevant Supervising Authority.

3.2 Identification of Sanctions Risk

The first step in performing an SRA is the identification of the sanctions-related risks to which the Operator may be exposed.

Operators should identify risks arising from their activities, products and services, customer base, geographic exposure, delivery channels and operational processes. Risks may also arise from the nature of transactions processed, the involvement of intermediaries or third parties and the jurisdictions connected to the Operator's business relationships.

By way of illustration:

- An Operator whose clients conduct business in jurisdictions subject to restrictive measures may face the risk that transactions involve sanctioned persons or activities;
- The use of intermediaries, agents or complex ownership structures may give rise to the risk that the involvement of designated persons is concealed; and
- Digital or remote onboarding channels may give rise to the risk that sanctions screening or identification controls are circumvented.

<u>Assessment of likelihood of each risk identified</u>

Once sanctions-related risks have been identified, Operators should assess the likelihood that each risk may materialise.

Likelihood refers to the probability that the Operator becomes exposed to a sanctions-related event, such as entering into a relationship with a designated person, processing a prohibited transaction or becoming involved in activities intended to circumvent restrictive measures.

When assessing likelihood, Operators should consider factors such as the nature of their clients, the jurisdictions connected to their business relationships, the complexity and frequency of transactions processed and the channels through which services are delivered.

For example, an Operator whose clients operate internationally and transact frequently with counterparties in multiple jurisdictions, may face a higher likelihood of sanctions exposure than an Operator whose activities are limited to domestic clients and transactions.

<u>Assessment of impact of each risk identified</u>

Operators should also assess the impact that a sanctions-related event could have, should the identified risk materialise.

Impact refers to the potential consequences for the Operator if a sanctions breach or circumvention event occurs. These consequences may include legal and regulatory penalties, financial losses, reputational damage and operational disruption.

When assessing impact, Operators should consider the potential severity of these consequences, taking into account factors such as the nature of the services provided, the scale of the Operator’s activities and the potential regulatory response to a breach.

For example, an Operator whose services facilitate large volumes of cross border transactions may face a higher potential impact in the event of a sanctions breach than an Operator whose activities are limited in scale.

The impact assessment should be documented and considered alongside the likelihood assessment when determining the inherent level of sanctions risk.

Calculation of inherent risk score

When assessing likelihood and impact, Operators should determine the inherent risk level associated with each identified risk.

Inherent risk reflects the level of risk to which an Operator is exposed before taking into account any mitigating controls. Operators will typically determine inherent risk by combining the likelihood and impact scores assigned to each identified risk. *Mapping of controls to risks.*

Operators should then identify and map the controls that are designed to mitigate each of the risks identified in the assessment.

These controls may include policies and procedures, customer due diligence measures, sanctions screening processes, transaction monitoring arrangements, escalation and reporting procedures, governance arrangements and training programmes and are further described in other Sections of this document.

Mapping controls to risks allows the Operator to understand how each risk is managed within its control framework.

Assessment of controls

Operators should assess the effectiveness of the controls identified in mitigating the relevant risks.

This assessment should consider both the design of the controls and their operational effectiveness. Controls that are poorly designed or inconsistently applied may not effectively mitigate the risks that they are intended to address.

Operators may draw on information from monitoring activities, internal assurance reviews, internal audit findings or compliance testing when evaluating control effectiveness.

Calculation of residual risk score

The final step is the determination of residual risk, which reflects the level of risk that remains after taking into account the mitigating effect of the Operator's controls.

Residual risk is determined by considering the inherent risk level together with the assessed effectiveness of the controls mapped to that risk.

This assessment allows Operators to identify areas where additional controls may be required and to ensure that sanctions-related risks are maintained within acceptable levels.

3.3 The SRA in the Context of the Sanctions Framework

The SRA should demonstrably inform the design and implementation of other controls in the Sanctions Framework (further described in the following Sections). Higher-risk exposures may require more robust or layered controls, while lower-risk activities may be managed through standard procedures and monitoring arrangements.

Operators are also required to ensure that mitigating measures are implemented effectively and operate as intended in practice. This requires periodic review of the performance of controls, including whether procedures are consistently applied, systems generate appropriate alerts, and escalation processes operate effectively.

In light of this requirement, Operators should ensure that a feedback mechanism through which the performance of controls informs the SRA on an ongoing basis. In other words, where monitoring, internal reviews, or operational experience indicate that controls are materially not functioning as expected, Operators should reassess the relevant risks and adjust their mitigating measures accordingly.

3.4 Timing of the SRA

Operators should conduct an SRA before commencing operations or introducing material changes to their activities. The purpose of the SRA is to identify and assess the sanctions-related risks to which the Operator may be exposed, and to ensure that appropriate controls are in place to mitigate those risks from the outset. This requirement applies in particular to:

New Operators

Operators that are commencing business activities should conduct an SRA prior to beginning operations. In such cases, the assessment will necessarily be forward-looking only and should be based on the Operator's intended activities, including the products and services it plans to offer, its target markets, the delivery channels it intends to use and its overall business model.

Existing Operators

Operators that are already established will typically be in a position to conduct their SRA with reference to both current and historical information.

In addition to considering their products, services, markets, delivery channels and business model, Operators should take into account information derived from their operational experience. This may include, for example, transaction patterns, client or counterparty behaviour, past compliance findings and any vulnerabilities identified through monitoring, assurance or audit activities.

Existing Operators Introducing Material Changes

Existing Operators should update their SRA before introducing material changes to their activities, business model or risk exposure. This may include, for example:

- The introduction of new products or services;
- Entry into new markets or jurisdictions;
- Changes to distribution channels or delivery technologies; or
- The adoption of a new or significantly-revised business model.

In such cases, the SRA should assess the sanctions risks associated with the proposed activities and consider how those risks may differ from those arising under the Operator's existing operating model.

3.5 Governance of the SRA

Clear ownership

Operators should ensure that clear responsibility is assigned for the preparation, maintenance and oversight of the SRA.

Senior management approval

The sanctions risk assessment must ultimately be reviewed and approved by senior management, the Board of Directors, or whichever level within the organisation carries ultimate business responsibility.

Integration with the control framework and decision-making

The SRA should be treated as an active component of the Operator's Sanctions Framework rather than a purely formal exercise and should be fully and effectively integrated within it. The outcomes of the SRA should inform the design of policies, procedures, and controls implemented to manage sanctions risk.

For additional information please see Chapter 12.

3.6 Documentation

Operators should ensure that the SRA is clearly documented.

Operators may choose either to integrate sanctions risk within their existing ML/FT framework or maintain a standalone sanctions risk assessment. Both approaches are acceptable, provided the sanctions risks relevant to the operator are properly identified, assessed, documented, and mitigated. Operators are afforded flexibility in relation to the methodology adopted, but not in relation to the quality or effectiveness of the assessment. Any methodology used should be clearly documented, proportionate to the nature, size, and complexity of the Operator's business and sanctions exposure, easy to follow, and capable of producing consistent and reliable results. Where weighting mechanisms are applied, Operators should also be able to explain how and why particular risk factors have been assigned specific weightings.

The documentation should describe the methodology used, the risk factors considered, the conclusions reached and the mitigating measures implemented to address the risks identified. The documentation should be sufficiently detailed to enable the Operator to demonstrate how sanctions risks arising from its activities have been assessed and managed.

The SRA and any supporting documentation should be maintained in a form that can be made available to the SMB, and to supervisors, upon request.

Operators should also ensure that documentation is updated when material changes occur in the Operator's activities, risk profile or control environment.

For additional information please see Chapter 8.

3.7 Reviewing and updating the SRA

Sanctions risks are dynamic and may change over time as the Operator's activities evolve or as sanctions regimes are updated. Operators should therefore ensure that the SRA is reviewed periodically at the appropriate frequency they deem necessary, depending on the size and complexity of the operator and the level of sanctions exposure involved. Operators integrating sanctions assessments within broader ML/FT frameworks may choose annual reviews, while others may determine that different review periods are proportionate to their circumstances. What is important is that the rationale adopted is properly documented within policies and procedures and that reassessments also occur whenever material changes arise that could affect sanctions exposure. Material changes that might occur that may affect the Operator's sanctions risk exposure may include:

- Significant changes to the Operator's business model, products or services;
- Expansion into new jurisdictions or markets;
- Changes in the Operator's client base or transaction profile; or
- Developments in applicable sanctions regimes.

Regular review of the SRA helps ensure that the Operator's Sanctions Framework remains aligned with its activities and continues to address the risks arising from applicable restrictive measures.

BORD TA' SORVELJANZA DWAR IS-SANZJONIJIET
SANCTIONS MONITORING BOARD
MALTA

Chapter 4

Customer Due Diligence

4. Customer Due Diligence (CDD)

At the heart of effective sanctions compliance is a clear understanding of the client and the parties connected to that client or to the relevant transaction. Without this understanding, Operators are not in a position to determine whether designated persons may be involved or whether sanctions exposure may arise.

In practice, this requires Operators to have in place processes to:

a. Identify clients and parties involved in a relationship or transaction whose involvement in the relationship or transaction may give rise to sanctions exposure;

b. Understand and verify ownership and control structures where legal persons or legal arrangements are involved;

c. Conduct sanctions screening against applicable sanctions lists;

d. Understand the context and objective of the relationship or transaction;

e. Assess the level of sanctions risk associated with a client or transaction;

f. Monitor the relationship on an ongoing manner for changes in sanctions exposure or sanctions risk

g. Repeat steps (a) to (e) when changes occur in a client or their relationship with them (e.g. changes ownership or control structures), and where new information becomes available that may affect sanctions exposure.

Collectively these processes are known as “Sanctions CDD”. While Sanctions CDD shares certain elements with AML customer due diligence, its objective is distinct. Its focus is on identifying connections to designated persons, sanctioned jurisdictions or prohibited activities, rather than on assessing broader money laundering risks. Sanctions CDD is a key component of an Operator’s Sanctions Framework. It enables Operators to understand the parties with whom they are dealing and to identify connections to persons, entities or jurisdictions subject to restrictive measures. The SMB expects Operators to implement Sanctions CDD effectively and to ensure that it is fully embedded within their operational procedures.

The following sections set out in greater detail the steps Operators should take to perform Sanctions CDD at different stages of a business relationship or transaction.

4.1 Determining Whether the Interaction Triggers Initial Sanctions CDD

The first stage at which Operators should consider the application of Sanctions CDD is at the outset of an interaction with a client.

Sanctions CDD should be applied before an Operator establishes a business relationship or carries out a transaction.

Accordingly, when interacting with a potential or existing client, Operators should first determine whether the interaction constitutes:

- The establishment of a business relationship; or
- The execution of a transaction, including a single or occasional transaction.
- In both circumstances, Sanctions CDD should be conducted.

This applies irrespective of the value of the transaction, and equally to ongoing client relationships and to single transactions.

Sanctions CDD should not be delayed until a business relationship has been formally established, or a transaction has been executed. Operators should ensure that the necessary checks are carried out sufficiently in advance to prevent the establishment of a relationship or the execution of a transaction involving a designated person before Sanction CDD has been complete.

It is particularly important where Operators offer payment terms to occasional transaction customers. In such circumstances, sanctions screening and CDD should be completed prior to the delivery of goods or the provision of services, rather than prior to invoicing.

Where screening is performed only at the invoicing stage, the Operator may already have supplied goods or provided services before identifying that the customer is subject to sanctions. This may expose the Operator to a breach of Article 9(e), (f) or (g) of the NIA, depending on the nature of the activity undertaken.

Where Operators apply the Simplified Due Diligence (SDD) exemption under the AML/CFT framework, they may also apply this approach to sanctions screening, subject to the same risk-based conditions and limitations. In such cases, onboarding may proceed for low-risk customers without undue delay; however, sanctions screening and any required identification and verification measures must still be completed as soon as reasonably practicable and within a defined timeframe following the establishment of the business relationship. The application of SDD, including where it permits the deferral of verification steps for low-risk clients and the associated strict time limits, should be clearly set out in the Operator's policies and procedures.

Examples of when initial Sanctions CDD is required

Sanctions CDD should normally be performed where an Operator is about to establish a business relationship or carry out a transaction. Examples include:

- A client applies to open an account or otherwise establish a business relationship with the Operator.

- An existing client requests the execution of a transaction, such as the purchase or sale of assets through the Operator.

Examples of when initial Sanctions CDD would not normally be required

Sanctions CDD would not normally be required where the interaction does not involve the establishment of a business relationship or the execution of a transaction. Examples include:

- A prospective client requests general information about the Operator's services but does not proceed with onboarding or engagement; or

- An individual attends an initial consultation or submits a preliminary enquiry solely to determine eligibility or obtain a fee estimate, without instructing the Operator to act.

4.2 Identifying the Universe of Parties Associated with the Relationship or Transaction

Having determined that Sanctions CDD is required, the next step for Operators is to determine which parties to screen against sanctions lists with a view to assessing whether any are subject to restrictive measures.

To achieve this, Operators should first determine the universe of parties associated with a client or a transaction. These fall in three categories:

- The client;
- Parties on behalf of whom the client is acting; and
- Other parties relevant to the relationship or transaction (such as beneficial owners and controllers but also, in certain circumstances, intermediaries, agents and counterparties).

Not all parties associated with a client or transaction will need to be screened (see Section 4.3 below) but understanding the key parties associated with a client relationship or transaction is an important step in ensuring that all relevant parties are then screened.

The level of analysis should be proportionate to the nature and complexity of the relationship or transaction. For straightforward relationships involving a natural person client and no intermediaries, the universe of parties may consist only of the client itself. Where the client is a legal entity or where the transaction involves multiple parties, additional persons may need to be considered.

Operators should be able to demonstrate that they have considered which parties are relevant for sanctions screening. This does not require a formal analysis in every case. However, Operators should maintain sufficient records, such as client files, ownership information or transaction documentation, to demonstrate a reasonable and proportionate approach.

4.2.1 The Client

The first party associated with the relationship or transaction is the client.

For the purposes of Sanctions CDD, the client is the natural or legal person that seeks to establish a business relationship with the Operator or to carry out a transaction with the Operator.

Accordingly, the client may include:

- A natural person seeking to establish a business relationship with the Operator;
- A legal person or legal arrangement entering into such a relationship;
- An existing client with whom the Operator already maintains a relationship; or
- A natural or legal person seeking to carry out a one-off transaction or a series of related transactions.

The client represents the primary counterparty to the relationship or transaction and therefore forms the starting point for determining the wider set of parties associated with the interaction.

Example – Client

A manufacturing company approaches an Operator to open an account and establish a business relationship in order to make international payments to its suppliers.

In this case, the manufacturing company is the client, as it is the legal person seeking to establish the relationship with the Operator.

Example – Not a client

An employee of the manufacturing company contacts the Operator to submit payment instructions on behalf of the company.

In this case, the employee is not the client. The employee is acting on behalf of the company, which remains the client.

4.2.2 Parties on Behalf of Whom the Client Acts

In some circumstances, the client may be acting on behalf of another person or entity.

This may be the case where the client is acting as an intermediary, agent, representative or other authorised person in a transaction that ultimately benefits another party.

In such cases, the person on whose behalf the client is acting should also be considered part of the universe of parties associated with the relationship or transaction.

Knowledge of such parties is important because sanctions exposure may arise from the underlying party benefiting from the transaction, rather than from the client interacting directly with the Operator.

Example

A trading company approaches an Operator to arrange payment for a shipment of goods. During the interaction, it becomes clear that the trading company is acting as an intermediary for another company that is the actual purchaser of the goods.

In this case, the trading company is the client, while the underlying purchaser is the party on whose behalf the client is acting.

4.2.3 Other Parties Relevant to the Relationship or Transaction

In addition to the client and any parties on whose behalf the client is acting, other persons or entities may be associated with a relationship or transaction in a way that could give rise to sanctions exposure.

This arises more frequently where the client is a legal person or legal arrangement, as such structures often involve multiple layers of ownership and control, as well as additional parties involved in governance or representation.

Determining parties that fall within this category will often require the greatest degree of judgement on the part of Operators.

Beneficial ownership and control

As we will see below, beneficial owners are a prominent type of party relevant to relationships and transactions for the purposes of sanctions risk, and one that must always be identified and should be screened.

Before discussing parties relevant to the transaction, a word on beneficial ownership.

A beneficial owner is defined as the natural person who ultimately owns or controls a legal entity.

Under EU (and therefore Maltese) AML/CTF regulation, firms are required to determine and verify the identity of beneficial owners that own more than 25% of shares or voting rights, or who exercise control through other means. That means that where a party does not have at least 25%+1 of shares or voting rights and does not exercise control through other means, firms have the option not to identify them.

Sanctions regulation does not apply this distinction. The sanctions test is not whether a person meets a beneficial ownership threshold, but whether an entity may be owned or controlled by a designated person. Ownership is defined as the possession of 50% or more of the proprietary rights of an entity or having majority interest in it. Because such possession is assessed in aggregate by all designated persons in an entity (for example, if one designated person owns 30% of the entity and another designated person owns 25% of the entity, then the entity should -, in principle - be considered as owned by designated persons.) it may be necessary for Operators to identify and screen all persons holding ownership interests in the entity, including shareholders whose interests fall below the AML/CTF beneficial ownership threshold.

It is important to remember, however, that beneficial ownership does not arise only from ownership of shares or voting rights but also from control. Control may exist where a person/entity:

- Has the right or power to appoint or remove a majority of the administrative, management, or supervisory body members

- Can appoint the majority of members serving in administrative, management, or supervisory bodies during the current and previous financial year

- Controls a majority of voting rights, whether acting alone or through an agreement with other shareholders or members

- Holds the right to exercise dominant influence over the legal person or entity through contractual agreements or provisions in the entity's Memorandum or Articles of Association (provided such provisions are legally valid under the governing law)

- Holds the power to exercise dominant influence (as described in the previous point) even if not the actual legal holder of that right

- Has the right to use all or part of the assets of the legal person or entity

- Manages the business on a unified basis, e.g., by publishing consolidated accounts

- Shares financial liabilities jointly and severally with the legal person or entity or acts as a guarantor for them.

These criteria are indicative, not exhaustive. Other circumstances may also demonstrate that control exists. For this reason, Operators should not limit their analysis to formal ownership thresholds alone and must maintain clear records of all efforts and steps taken to identify beneficial ownership and control.

Parties relevant to the relationship or transaction

Such parties that Operators should treat as relevant to the relationship or transaction and consider for screening are:

- Persons holding shares, equity or other ownership rights in the client directly;

- Persons holding shares, equity or other or ownership rights in the client indirectly, including through one or more intermediate entities in the ownership chain;

- Persons exercising control over the client, including through governance rights, debt, contractual arrangements or other mechanisms capable of conferring dominant influence. For example, in the context of a trust, this could be a person having the powers to dispose of, advance, lend, invest, pay or apply trust property, vary or terminate the trust, add or remove a person as a beneficiary or to or from a class of beneficiaries, appoint or remove trustees or give another individual control over the trust. That person could also direct, withhold consent to or veto the exercise of a power mentioned in the previous sentence, and which powers typically are held by the trustee or possibly a protector, albeit sometimes (to some degree or other) retained by the settlor or other named person in the trust instrument);

- Beneficial owners of legal arrangements, such as foundations or associations including: the founder; the administrator (s;, the guardian, protector or members of the supervisory council; the beneficiaries or the class of persons in whose main interest the foundation or association is set up; and any other natural person exercising ultimate control over the foundation by means of direct or indirect ownership, or by any other means. The reference to the founder should not be construed as being limited to the original founder but is also to include any other person who makes subsequent endowments to the foundation or is otherwise assigned any rights of a founder.

- Beneficial owners of legal arrangements such as - and similar to - trusts, including: the settlor; the trustee(s); the protector; where applicable (as not all trusts have a protector or equivalent), the beneficiaries, regardless of the extent of their beneficial interest; or, where the beneficiaries have yet to be determined, the class of persons in whose main interest the trust is established or operates; and any other natural person exercising ultimate control over the trust through direct or indirect ownership or by other means.

  The settlor should not be construed as being limited to the original settlor, but should include also any other person who, subsequent to the creation of the trust, adds property to the trust settlement.

- Beneficial owners of partnership *en nom collectif* including all partners (given that each partner is jointly and severally liable for the obligations of the partnership) and any other natural person exercising ultimate control over the partnership by means of direct or indirect ownership, or by any other means. Unless otherwise provided in the partnership deed, each partner has the authority to administer and represent the partnership. As a result, all partners in a partnership *en nom collectif* are generally considered to exercise control over the partnership and should therefore be identified as beneficial owners for sanctions due diligence purposes.

- Beneficial owners of commercial partnerships. In this case identification of beneficial owners and persons exercising control will depend on the type of partnership and the rights and obligations of the partners as established by law and by the partnership deed.

- Beneficial owners of partnership *en commandite*, including: the general partners (given their unlimited, joint and several liability and their authority to administer and represent the partnership); limited partners (where they hold a significant ownership or economic interest in the partnership); and any other natural person exercising ultimate control over the partnership by means of direct or indirect ownership, or by any other means. General partners are responsible for the administration and representation of the partnership, unless otherwise provided in the partnership deed, and should therefore be regarded as exercising control. Limited partners are generally not involved in the administration or representation of the partnership and are liable only up to the amount of their agreed contribution. However, limited partners may still qualify as beneficial owners where they hold a significant participation or where the partnership deed or any other arrangement grants them decision-making powers, veto rights, or other forms of control. Operators should carefully review the partnership deed and any related agreements, as these may alter the default legal position regarding management, representation, ownership, or control.

- Shareholders or parent entities within the ownership structure of the client. These entities may hold ownership interests in the client directly or indirectly. Understanding the broader ownership structure enables Operators to determine whether a designated person may hold an ownership interest through intermediate entities.

- Intermediaries, agents or brokers involved in facilitating the relationship or transaction. Transactions may involve intermediaries, such as agents, brokers, introducers or other representatives. These parties may facilitate the relationship between the Operator and the underlying parties to the transaction. In some cases, intermediaries may be acting on behalf of another party or may introduce clients to the Operator. Operators should therefore consider whether intermediaries are involved and whether their participation may create sanctions exposure.

- Counterparties to the transaction, such as buyers, sellers or service providers may include buyers, sellers, suppliers or service providers that are party to the transaction being carried out through the Operator. Where funds, goods or services are transferred to another party, that party may create sanctions exposure even where the client itself is not subject to sanctions

- Other persons or entities directly participating in the transaction, where their involvement may give rise to sanctions exposure. This may include financial intermediaries, logistics providers, escrow agents or other parties whose involvement forms part of the transaction structure. Operators should consider whether such parties are involved and whether their participation could result in funds or economic resources being made available to a designated person; and

- Minority shareholders. Where the client is a legal person, Operators may encounter shareholders who hold minority ownership interests in the entity. Minority ownership interests do not, by themselves, create sanctions exposure. However, Operators should remain alert to situations where a designated person may hold multiple minority interests that could collectively meet the relevant sanctions ownership thresholds. Operators should also consider whether a minority shareholder may nevertheless exercise control over the entity through other means, such as voting arrangements, contractual rights or governance structures.

<u>Entities Not Established for the Benefit of Identifiable Beneficiaries</u>

Some legal entities or legal arrangements may not be established for the benefit of identifiable beneficiaries, but rather to pursue a specific purpose or cause. In such cases, there may be no beneficiaries to identify. Examples of such legal entities or arrangements are Trusts, Associations and Foundations.

Operators should nevertheless:

- Consider for screening other relevant parities such as persons exercising control or governance, persons acting on behalf of the entity and transaction counterparties; and

- Establish the purpose for which the entity or arrangement has been established and assess whether this purpose is consistent with the nature of the relationship or transaction. This assists Operators in understanding the context in which it operates, whether its activities are consistent with the relationship or transaction being undertaken and to assess whether the structure could nevertheless be used to make funds or economic resources available - directly or indirectly - to a designated person.

4.3 Determining Parties to Screen

Once the universe of parties associated with the relationship or transaction has been identified, Operators should consider which of those parties should be screened against applicable sanctions lists.

The purpose of screening is to determine whether a designated person is involved in, benefits from, or exercises ownership or control over the relationship or transaction. Screening should therefore focus on parties whose involvement could give rise to sanctions exposure.

While Article 32(1)(b) does not expressly identify the categories of persons or entities to be screened, Operators remain subject to the overarching obligation to ensure that funds or economic resources are not made available, directly or indirectly, to designated persons or to entities owned or controlled by them. Screening is a key control used to support compliance with this obligation.

Operators should therefore distinguish between identifying parties associated with a relationship or transaction and determining which of those parties should be screened.

In practice, Operators may need to identify ownership and control broadly in order to understand whether a designated person could be involved. However, the decision as to which of those parties should be screened should be risk-based and proportionate, taking into account the likelihood that a party's involvement could give rise to sanctions exposure.

In practical terms, Operators should ask ***if this party were designated, would we be breaching our obligation not to make resources available to them, directly or indirectly?***

Where the answer is "yes", the party should be screened.

In practice, a party that is a designated entity could put the Operator in breach of the obligation not to make resources available, directly or indirectly, to designated persons or to entities owned or controlled by them if:

a. the party were the direct client of the Operator;

b. the party were the owner of the client of the Operator (i.e. someone who possesses 50% or more of the ownership, voting or proprietary rights of an entity, or a majority interest in it) either solely or in aggregate with others);

c. the party were the controller of the client of the Operator; or

d. other mechanisms (e.g. payment of dividends or distributions, or transfer of assets) exist through which the client of the Operator could make funds or economic resources available to a designated person.

Shareholders of private companies

In relation to (d), in the case of private companies, where a shareholder is a designated person but does not meet the relevant ownership threshold and does not exercise control over the company, the client of the Operator would not be considered owned or controlled by a designated person. In such circumstances, this would not automatically prevent the Operator from onboarding the client or providing services to it.

The Operator must ensure, however, that it does not make funds or economic resources available to the designated shareholder (through payment of dividends, distributions of profits or transfers of assets or value to the shareholder). If the Operator's services were to facilitate such payments, those payments could be prohibited. In some cases, the client relationship may still be possible if the Operator is capable of ensuring that its own services do not result in funds or economic resources being made available to the designated shareholder. If the Operator cannot prevent funds or economic resources from being made available to the designated shareholder, then the Operator would not be able to onboard the client without breaching sanctions obligations.

Determining whether sufficient safeguards can be put in place, and what those safeguards may be, are beyond the scope of this Guidance Note and would typically require legal counsel or the engagement of specialised compliance consultants.

For the purposes of determining whether or not to screen a party who is a shareholder or might receive value from a client, Operators should consider risk, risk appetite and proportionality. For example, an Operator might take the view that screening a single shareholder would be straightforward and, therefore, proportionate, but screening hundreds of small investors (such as in the case of a fund with hundreds of limited partners or a company with hundreds of shareholders, each holding very small passive stakes, with no governance rights, and unable to exercise control or trigger the 50 percent rule) might be disproportionate to the risk represented to the Operator. However, the Operator should recognise that choosing not to screen those parties would result in the Operator assuming the residual risk associated with that decision.

Shareholders of companies that are listed on Stock Exchanges

Operators are not required to identify or screen the shareholders of companies publicly listed on regulated markets within the European Economic Area ("EEA") that are included in the register of regulated markets maintained by the European Securities and Markets Authority ("ESMA").

For companies listed on non-EEA stock markets, Operators must take reasonable steps to ascertain that the jurisdiction in which the market is located is reputable and that the market is subject to regulation comparable to that applicable to regulated markets within the EEA.

Before relying on this exemption, Operators should consider whether any sanctions have been imposed on the jurisdiction in question and whether any regulatory actions have been taken by the relevant supervisory authority or the regulated market against the listed company for breaches of disclosure obligations. A record of the checks performed should be retained in the client file.

In essence, there are three different screening rationales:

- Ownership risk - The client may itself be considered sanctioned if a designated persons own ≥50%.

- Control risk - The client may be considered sanctioned if a designated person controls it.

- Funds flow risk - The Operator may make funds available to a designated person (for example through dividends).

Operators should assess and consider each screening rationale independently, as well as their cumulative effect in order to decide whether or not to screen a party.

Important note

In Annex II we provide guidance as to parties that Operators should ordinarily screen (because they are, or have a great likelihood to be, in one of the three categories described above) and also those that should instead be screened where relevant. Worked examples are included to illustrate how these principles may apply in practice.

This is intended as directional guidance. Operators should note that precise determination of which parties to screen will need to be made on a case-by-case basis, having regard to the nature of the relationship or transaction, and to the sanctions exposure that may arise.

4.3.1 Parties That Operators Should Ordinarily Screen

Operators should ordinarily screen, at a minimum:

- The client;
- Beneficial owners of the client; and
- Persons exercising control over the client.

These parties should always be screened because sanctions measures may apply where a designated person owns or controls an entity, even where that entity itself does not appear on a sanctions list.

4.3.2 Parties That Should Be Screened Where Relevant

Operators should also screen other parties where their involvement in the relationship or transaction may create sanctions exposure. These may include:

- Material shareholders;
- Minority shareholders where there are indicators of control;

- Persons acting on behalf of the client, such as agents, authorised representatives or legal intermediaries;
- Intermediaries, agents or brokers involved in facilitating the transaction;
- Counterparties to the transaction, such as buyers, sellers or service providers; and
- Other persons or entities directly participating in the transaction where their involvement may result in funds or economic resources being made available to a designated person.

Operators are generally not expected to screen every person associated with a client or corporate structure. For example, it will not normally be necessary to screen:

- Minority shareholders who do not exercise ownership or control;
- All directors or employees of a client where their involvement does not create sanctions exposure; or
- Every entity within a wider corporate group where those entities neither own nor control the client and are not involved in the transaction.

Operators should bear in mind that their obligation is outcome-based. They must ensure that they do not make funds or economic resources available, directly or indirectly, to a designated person and must ensure they are not dealing with assets of a designated person.

Operators should make a determination as to whether to screen certain parties depending on the nature of the relationship or transaction, and on the extent to which they are involved in the movement of funds, goods or services.

<u>Example of when screening is required</u>

A trading company instructs an Operator to process a payment to a supplier for the purchase of goods. The transaction involves:

- The trading company (the client);

- The supplier receiving payment; and

- A broker facilitating the transaction.

Because the supplier and the broker are directly involved in the transaction and may receive or influence the flow of funds, the Operator should screen both of these parties in addition to the client.

Example of when screening is not typically required

A manufacturing company is the client of the Operator. The company has a large number of employees and several external professional advisers, such as auditors and consultants. These persons are not involved in the transaction being conducted through the Operator and do not receive funds from or exercise control over the client.

In this situation, it would not normally be necessary to screen all employees or advisers, as their involvement does not create sanctions exposure.]

For some more complex examples in practice, see Annex II.

4.4 Obtaining Identifying and Verifying Information

To screen parties, Operators should obtain sufficient identifying information. The objective is not to collect information for its own sake, but to ensure that the Operator can conduct sanctions screening with sufficient certainty and distinguish the person from other individuals or entities with similar names.

The information obtained typically includes:

For natural persons:

- Full name;

- Date of birth;

- Nationality; and

- Residential address or country of residence.

For legal persons:

- Legal name of the entity;
- Jurisdiction of incorporation or establishment;
- Registration number or equivalent identifier; and
- Registered or principal place of business.

Operators should obtain this information from reliable sources, such as official identification documents, company registries, constitutional documents, or other credible and independent sources.

In most circumstances, documentation already collected for AML/CFT purposes may also satisfy sanctions-related verification requirements. However, where sanctions regulations prescribe specific documentation requirements, those requirements take precedence.

For example, Article 5b(2) and 5b(3) of Council Regulation 833/2014 prohibits the provision, directly or indirectly, of crypto-asset services and payment or electronic money services to Russian nationals, residents, or legal persons, entities or bodies established in Russia, unless they provide evidence of EU, EEA or Swiss nationality or a valid EU, EEA or Swiss residence permit (temporary or permanent). In such cases, only a valid EU, EEA or Swiss passport or a valid EU, EEA or Swiss residence card is considered acceptable evidence for compliance purposes. Accordingly, Operators should continuously monitor developments in applicable sanctions legislation and ensure that internal policies, procedures and controls are updated in a timely manner to reflect any changes in legal obligations.

4.5 Inability to Obtain Identifying Information about the Client or Other Parties Relevant to the Transaction

Where the Operator is unable to obtain sufficient identifying information about the client or relevant parties, the Operator should consider whether or not it might be possible to establish the business relationship or execute the transaction. We distinguish between two cases:

- Where it is not possible to obtain sufficient identifying information about the client, the beneficial owner(s) of the client or parties exercising control over the client, the Operator must not proceed to establish the business relationship or execute the transaction (as proceeding without such information would be in breach of Article 32 (1)(a) of the NIA).

The SMB is aware of instances where Operators have proceeded despite incomplete or insufficient identification of the client, beneficial owner(s) or persons exercising control. Such practices are not consistent with the obligations set out above.

In the context of supervisory engagement or enforcement action, Operators should be able to demonstrate:

- What information was obtained at the time of onboarding;
- What information was missing;
- What steps were taken to obtain it; and
- The basis on which the decision to proceed was taken.

The absence of such documentation may be taken into account as an aggravating factor.

- Where it is not possible to obtain sufficient identifying information about parties to the transaction other than the client, the beneficial owner(s) of the client or parties exercising control over the client, Operator should consider sanctions risks and exposure before proceeding to establish the business relationship or execute the transaction. The Operator should not establish the business relationship or execute the transaction unless it can otherwise satisfy itself, on the basis of reliable information, that no funds or economic resources will be made available, directly or indirectly, to a designated person or to an entity owned or controlled by one.

Where, in exceptional circumstances, the Operator proceeds despite incomplete identification of parties other than the client, beneficial owner(s) or controller(s), the Operator should clearly document:

- the information that could not be obtained;
- the steps taken to obtain that information;
- the reasons why those steps were unsuccessful;
- the alternative sources of information relied upon; and
- the basis on which the Operator satisfied itself that proceeding would not result in funds or economic resources being made available, directly or indirectly, to a designated person.

Such documentation does not, in itself, mitigate or remove the Operator’s obligations under applicable sanctions regimes. Operators remain responsible for ensuring compliance with Article 5 of the NIA and for being able to demonstrate that their decision to proceed was reasonable and justified in light of the information available at the time.

Operators should also remain alert to situations where a (prospective) client is reluctant to provide information, delays providing documentation, or provides information that appears incomplete, inconsistent or unreliable. These behaviours may indicate elevated sanctions risk or an attempt to conceal the identity of a party involved in the relationship or transaction. This may happen whilst verifying ownership or control structures that appear unclear or unusually complex.

In such circumstances, Operators should take reasonable steps to clarify the situation before proceeding. This may include:

- Requesting additional documentation or explanations from the client;
- Obtaining information from independent or reliable sources such as company registries, official identification documents or publicly available records;
- Seeking clarification regarding the role of intermediaries or other parties involved in the transaction.

Operators should exercise particular caution where:

- The client is unable or unwilling to explain ownership or control structures;
- Different documents provide conflicting information about the parties involved;
- Information appears deliberately vague or incomplete; or
- The client attempts to proceed with the transaction before the Operator has completed its due diligence.

Where reasonable steps to clarify the situation do not resolve the uncertainty, the Operator should decline to establish the business relationship or execute the transaction.

Operators should ensure that the reasons for refusing or discontinuing the relationship are appropriately documented.

Please note: A refusal to establish the relationship due to insufficient information does not automatically trigger a reporting obligation to the SMB as a suspected violation under Article 32(1)(e) of the NIA. A report may, however, become appropriate if the circumstances create a reasonable suspicion of sanctions circumvention or of a breach of restrictive measures.

4.6 Screening and Reviewing Potential Matches

Once the Operator has obtained sufficient identifying information for the relevant parties, the next step is to conduct sanctions screening. Sanctions screening involves comparing the identifying information of the parties identified in the previous sections against applicable sanctions lists. The objective is to determine whether any party to the relationship or transaction is a designated person or entity subject to restrictive measures.

Operators should screen relevant parties against applicable restrictive measures, including those adopted by the UN Security Council, EU and any domestic designations issued under Maltese law.

In practice, sanctions screening is often carried out using automated screening systems that compare the identifying details of relevant parties against applicable sanctions lists. Automated systems are generally appropriate where Operators process a high volume of clients or transactions or where screening must be performed on a frequent basis.

However, automated solutions are not mandatory in all cases. Operators may perform sanctions screening manually, provided that the approach adopted remains effective and proportionate to the nature, size and complexity of their activities.

Where manual screening is used, Operators should ensure that procedures are sufficiently robust to enable reliable identification of potential matches and that screening is carried out consistently and in a timely manner and accurately documented. Regardless of whether screening is automated or manual, Operators remain responsible for ensuring that their screening processes are capable of identifying designated persons and preventing funds or economic resources from being made available to them.

Sanctions screening will produce potential matches where the identifying details of a screened party correspond, wholly or partially, with those of a person or entity appearing on a sanctions list. Not all potential matches represent designated persons. In many cases, matches arise because individuals or entities share similar names or identifying details. Operators should therefore review potential matches to determine whether the match represents a true match or a false positive.

When reviewing a potential match, Operators should compare the identifying information obtained during due diligence with the information contained in the sanctions listing. Relevant identifying details may include:

- Full name and known aliases;
- Date and place of birth (for natural persons);
- Nationality or country of residence;
- Addresses; and

- Corporate identifiers such as registration numbers or jurisdictions of incorporation.

Where the available information clearly indicates that the screened party is not the same person or entity as the designated person, the Operator may conclude that the match is a false positive. The Operator should record the basis for this conclusion.
Where the available information is insufficient to determine whether the match is genuine, the Operator should take reasonable steps to obtain additional information from reliable sources. This may include requesting further information from the client or consulting independent sources such as company registries or other public records.

4.7 Outcomes of Sanction Screening

Once potential matches have been reviewed, Operators should determine the outcome of the sanctions screening process.

In practice, screening will lead to one of three outcomes:

- No party is a confirmed match to a designated person;
- A party is a designated person, but the ownership or control thresholds are not met; or
- A party is a designated person, and the relevant ownership or control thresholds are met.

The appropriate course of action will depend on which of these outcomes applies.

4.7.1 When No Party is a Confirmed Match to a Designated Person

Where the screening process confirms that none of the parties associated with the relationship or transaction corresponds to a designated person, the Operator may proceed with the next steps of the sanctions due diligence process. This will typically involve carrying out a Sanctions Customer Risk Assessment ("CRA", see Section 4.8 for details) and applying monitoring and control measures proportionate to the sanctions risk associated with the client.

4.7.2 When a Party is a Designated Person, but the Ownership Threshold is Not Met

In some circumstances, sanctions screening may identify a designated person associated with the relationship or transaction, but the relevant ownership or control thresholds are not met.

For example, a designated person may hold a minority ownership interest in the client that does not meet the threshold required for the entity itself to become subject to sanctions measures. In such cases, the Operator may proceed with the relationship or transaction provided that no sanctions prohibitions apply.

However, the presence of a designated person in the ownership or control structure may indicate elevated sanctions risk. Operators should therefore take this factor into account when performing a CRA and determining the level of monitoring or additional controls required.

4.7.3 When a Party is a Designated Person, and the Ownership Threshold is Met

Where sanctions screening confirms that a designated person owns or controls the client or another relevant party in a manner that triggers the applicable sanctions measures, the Operator must not proceed with the relationship or transaction.

Operators must therefore ensure that they do not make funds or economic resources available to the entity, directly or indirectly.

Operators should also comply with any applicable freezing and reporting obligations, including reporting the matter to the SMB.

If a designated person is identified prior to onboarding or the execution of a transaction, and engagement is refused on the basis of sanctions concerns, the Operator should inform the SMB of the attempted action, in accordance with Article 32(1)(d) and (e). Details on how to report to the SMB are set out in Chapter 5.

4.7.4 Is the Ownership Threshold Met?

In determining whether the Ownership Threshold is met, Operators should assess whether designated persons hold 50 percent or more of the proprietary rights in the entity, either directly or indirectly.

In practice, this requires Operators to aggregate the ownership interests of designated persons where more than one designated person holds an interest in the same entity. For example:

- Designated Person A owns 30% of Company X.

- Designated Person B owns 25% of Company X

.
The combined ownership by designated persons is 55%, meaning Company X would generally be treated as owned by designated persons.

Where ownership is held through intermediate entities, Operators should trace the ownership chain to determine whether effective ownership by designated persons in the entity meets the 50 percent threshold.

Where an operator screens only a portion of the individuals within a client's ownership structure and identifies a designated person holding less than 50% of the shares, the operator must proceed to screen all persons within the structure. This is to ensure that no other designated person is involved whose shareholding, individually or in aggregate with other designated persons, amounts to 50% or more of ownership or control. If, after screening all individuals within the structure, the identified designated persons collectively hold less than 50%, the client may be serviced, provided that a board resolution from the client is obtained confirming that no funds or economic resources will be made available to any designated person. The operator must inform the SMB accordingly and keep it updated in the event of any subsequent developments.

4.7.5 Ownership vs Control

Where a person who controls the client is a designated person, the Operator must not proceed with the relationship or transaction. In such circumstances, the Operator must ensure that no funds or economic resources are made available to the entity, directly or indirectly. This applies even where the designated person does not meet the ownership threshold. Control over the entity is sufficient for the restrictive measures to apply and is not subject to thresholds. Operators should therefore assess both ownership and control when determining whether sanctions measures extend to the client or to another relevant party.

4.8 Customer Risk Assessment

Having completed sanctions screening, Operators should assess the level of risk associated with each client. This process is referred to as a Sanctions CRA. Similarly to the SRA, Operators, particularly those relying on automated systems, may utilize a single risk rating model for both ML/FT and sanctions purposes. Of course, the ultimate client risk would then indicate an all-encompassing financial crime and sanctions risk.

If the CRA is conducted separately, the Operator will find it easier to determine the extent to which a client may expose them to risks of sanctions breaches or circumvention of restrictive measures.

Irrespective of whether the CRA is applied separately or integrally within the ML/FT framework, the assessment must still appropriately account for sanctions-specific risk factors associated with the client, based on the five pillars. These factors will typically include:

- *Ownership and control structures* - The transparency and complexity of the client's ownership structure, including the identification of beneficial owners, shareholders and controllers. Opaque or complex structures may increase the risk that designated persons are concealed within the ownership chain;

- *Geographical exposure* - The jurisdictions connected to the client, including the country of incorporation, residence, operation or transaction flows. Connections to sanctioned jurisdictions or jurisdictions associated with sanctions circumvention may increase sanctions risk;

- *Nature of the client's activities* - The sectors in which the client operates and whether these sectors are commonly exposed to sanctions risks, such as energy, shipping, defence, commodities or trade involving dual-use goods;

- *Products and services used* - The products or services that the client intends to use and the extent to which these may involve cross-border transactions, trade flows, financial transfers or other activities that may create sanctions exposure; and

- *Transaction profile* - The expected nature, frequency and value of transactions associated with the relationship and whether these are consistent with the client's stated business activities.

In performing the CRA, Operators may need to obtain additional information about the client, the client's activities, and the nature of the transaction in order properly to assess the sanctions risks associated with the relationship.

The CRA should result in the assignment of a risk rating for the client. Operators may use risk categories such as low, medium, or high risk, or another internally defined risk classification system.

The risk rating should reflect the overall sanctions exposure presented by the client after considering the relevant risk factors.

- The assigned risk rating should guide the level of scrutiny applied to the relationship, including:

- The frequency and intensity of monitoring; and

- The level of internal oversight required.

Higher-risk clients may require additional approvals before onboarding, or more frequent monitoring of transactions and activities.

4.9 Enhanced Due Diligence

The sanctions risk associated with a client, relationship or transaction may require Operators to obtain and assess information beyond that required for standard Sanctions CDD. This is referred to as Enhanced Due Diligence ("EDD").

EDD is not a separate process from Sanctions CDD. It is the application of additional or more intensive due diligence measures where the information obtained through Sanctions CDD, sanctions screening, the CRA, adverse media, ongoing monitoring or other relevant sources indicates elevated sanctions risk or uncertainty.

The purpose of EDD is to enable Operators to understand more fully whether the relationship or transaction may involve a designated person, an entity owned or controlled by a designated person, a sanctioned jurisdiction, a prohibited activity, or an attempt to breach or circumvent restrictive measures.

<u>When EDD should be required</u> - Operators should apply EDD where the sanctions risk associated with a client, relationship or transaction is assessed as high or where standard Sanctions CDD identifies unresolved sanctions related risk factors requiring further verification before the Operator can reasonably conclude that funds or economic resources will not be made available, directly or indirectly to a designated person or to an entity owned or controlled by one. EDD should normally be required where:

- The CRA results in a high risk rating;
- The client has material connections to a jurisdiction subject to restrictive measures or to a jurisdiction associated with sanctions circumvention;
- The client's ownership or control structure is complex, opaque, unusually layered or otherwise difficult to understand;
- There is a high degree of uncertainty as to whether a designated person may hold an ownership interest in, or exercise control over, the client or another relevant party;
- The client, beneficial owner, controller, counterparty, intermediary or other relevant party is connected to sectors or activities that may create elevated

sanctions exposure, including sectors subject to trade, transport or financial restrictions;

- The relationship or transaction involves intermediaries, agents, brokers or other third parties whose role is not clear or whose involvement may obscure the identity of the person ultimately benefiting from the relationship or transaction;

- The transaction involves goods, services, vessels, aircraft, payment flows or counterparties connected to jurisdictions, sectors or activities that present elevated sanctions risk;

- Adverse media or other information suggests a possible connection to sanctions breaches, attempts to circumvent restrictive measures, or indirect ownership or control by a designated person;

- Information provided by the client is incomplete, inconsistent, unreliable or difficult to verify;

- Situations where a party is not itself designated, but has a known connection with a designated person, a sanctioned jurisdiction, or activities that may be subject to restrictive measures;

- The client is reluctant to provide information, delays providing documentation, or seeks to proceed before the Operator has completed Sanctions CDD; or

- Ongoing monitoring identifies changes in the relationship, transaction profile, ownership structure or other circumstances that may increase sanctions risk.

<u>Where EDD May be necessary</u> - EDD may also be necessary in circumstances that do not automatically result in a high sanctions risk rating, but where additional information is needed to allow the Operator to understand and manage the sanctions exposure presented by the relationship or transaction. This may include, for example:

- Transactions involving new or unusual counterparties whose role in the transaction is not immediately clear;

- Relationships where the client operates in, trades with, sources goods from or makes payments to jurisdictions that may be relevant to sanctions exposure;

- Legal persons or legal arrangements where the identity of persons exercising control is not apparent from standard ownership information;

- Fund, trust, foundation or partnership structures where the rights of investors, beneficiaries, protectors, trustees, partners or other parties may affect ownership or control;

- Transactions involving changes in payment routes, delivery routes, counterparties or documentation that are inconsistent with the Operator's understanding of the client or transaction; and

- Cases where the Operator has decided not to screen certain associated parties on proportionality grounds but considers that additional information or controls are needed to manage the residual risk arising from that decision.

Nature of EDD measures - The EDD measures applied should be proportionate to the nature and level of sanctions risk identified. Depending on the circumstances, EDD may include:

- Obtaining additional information about the client's ownership and control structure;

- Identifying and, where appropriate, screening additional parties associated with the relationship or transaction;

- Obtaining further information about the client's business activities, transaction profile, expected counterparties and jurisdictions connected to the relationship or transaction;

- Obtaining further information about the purpose, expected activity and economic rationale of the relationship or transaction;

- Considering whether additional restrictions, controls or monitoring arrangements are required before the relationship or transaction may proceed;

- Applying more frequent or more detailed transaction monitoring;

- Requiring approval from an appropriate level of senior management or from a designated sanctions compliance function before onboarding the client or proceeding with the transaction; and

- Seeking legal advice where the Operator is unable to determine whether a sanctions prohibition may apply.

EDD should not be treated as a means of proceeding with a relationship or transaction where the Operator has not obtained sufficient information to understand sanctions exposure. Where, after applying EDD, the Operator is still unable to determine that the relationship or transaction complies with applicable sanctions obligations, the Operator should neither establish the relationship nor execute the transaction.

<u>EDD during the relationship</u> - EDD may be required at onboarding, before the execution of a transaction, or during the life of a business relationship.

Operators should consider whether EDD is required when new information becomes available, when there are changes to ownership or control, when the client's activities or transaction profile changes, when sanctions lists or restrictive measures are updated, or when monitoring identifies facts or circumstances that may increase sanctions risk.

Where EDD is applied during an existing relationship, Operators should consider whether the relationship may continue while the additional enquiries are being completed. This assessment should take into account the nature of the risk identified and whether continuing to provide services could result in funds or economic resources being made available, directly or indirectly, to a designated person or to an entity owned or controlled by one.

<u>Documentation and governance</u>

Operators should document the basis on which EDD was required or considered necessary, the measures applied, the information obtained, the outcome of the assessment and the decision reached. The documentation should be sufficient to demonstrate that the Operator has considered the sanctions exposure presented by the relationship or transaction and has taken reasonable and proportionate steps to address it.

Where the Operator proceeds with a relationship or transaction following EDD, the reasons for doing so should be recorded, together with any restrictions, approvals, monitoring requirements or other mitigating measures applied. Where the Operator declines or terminates a relationship or transaction following EDD, the reasons for that decision should also be documented. For additional information please see Section 8.

4.10 Adverse Media

Adverse media may provide relevant information when assessing sanctions risks. It can assist Operators in identifying facts or circumstances that may not be evident from customer due diligence information alone.

In particular, adverse media may reveal indicators relevant to sanctions exposure, such as potential indirect ownership or control of assets by designated persons, or connections between a client and third parties involved in sanctions breaches or circumvention.

The presence of adverse media should be treated as a potential risk indicator and considered as part of the overall assessment of a client or transaction, unless the information can reasonably be determined to be inaccurate or unreliable.

Where adverse media is identified, Operators should take reasonable steps to verify the information by consulting additional sources where appropriate.

The SMB encourages Operators to consider adverse media as part of their Sanctions CDD. Depending on the nature and credibility of the information identified, adverse media may also influence a decision to establish or continue a business relationship, even where the information is not directly related to sanctions.

4.11 Ongoing Monitoring

Sanctions CDD does not end once a client has been onboarded or a transaction has been completed. Operators should perform ongoing monitoring to ensure that the client, the parties associated with the relationship, and the transactions conducted through the Operator do not become subject to restrictive measures over time.

Ongoing monitoring enables Operators to identify changes in sanctions exposure that may arise after the initial due diligence has been completed. These changes may result from updates to sanctions lists, changes in the client's circumstances, or developments in the nature of the relationship or transaction.

Ongoing monitoring should therefore include, at a minimum:

- Repeating sanctions screening;
- Maintaining customer due diligence information up-to-date;
- Performing transaction monitoring; and
- Reviewing the customer risk rating.

4.11.1 Repeating Sanctions Screening

Operators should ensure that sanctions screening is repeated periodically in order to detect new designations. This is particularly important because sanctions lists are updated regularly. A person who was not designated at the time of onboarding may subsequently become subject to restrictive measures.

Operators should therefore ensure that relevant parties are re-screened when:

- Sanctions lists are updated;
- New information becomes available regarding the client or associated parties;
- Changes occur in the relationship or transaction.

Re-screening may be performed automatically where automated screening systems are used. Where screening is conducted manually, Operators should ensure that updates to sanctions lists are reviewed in a timely manner.

4.11.2 Maintaining Customer Due Diligence Information Up to Date

Operators should ensure that the information obtained during the Sanctions CDD process remains accurate and up-to-date throughout the relationship.

This includes information relating to:

- The identity of the client;
- Beneficial owners;
- Persons exercising control over the client; and
- Other relevant parties associated with the relationship or transaction.

Where changes occur in ownership structures, control arrangements, or other relevant circumstances, Operators should update their records and reassess the sanctions exposure associated with the relationship.

4.11.3 Transaction Monitoring

Transaction monitoring is an important component of sanctions compliance because sanctions risk may arise not only at the point of onboarding but also through the transactions conducted over the course of a business relationship. Even where appropriate due diligence and screening have been performed, transactions may involve new counterparties, sanctioned jurisdictions, or structures designed to obscure the involvement of designated persons. Ongoing monitoring of transactions therefore helps Operators identify situations where funds or economic resources may be made available, directly or indirectly, to designated persons or where restrictive measures may otherwise be breached.

Operators should monitor transactions carried out through their relationships with clients in order to identify potential sanctions exposure, remaining particularly alert to transactions involving:

- Sanctioned jurisdictions;
- Parties not previously associated with the relationship;
- Unusual routing of funds or the involvement of multiple intermediaries; and
- Transaction patterns that may indicate attempts to circumvent restrictive measures.

Where such indicators are identified, Operators should conduct further review to determine whether sanctions exposure may arise and take appropriate action where necessary.

Transaction monitoring may be carried out through a combination of automated systems and manual review processes. While automated tools can assist in analysing large volumes of transactions and identifying predefined risk indicators, Operators should ensure that appropriate manual oversight and investigation processes are in place to assess alerts and determine whether sanctions exposure may arise.

The types of red flags to which Operators should remain alert through automated transaction monitoring and/or manual review of transactions include, for example:

- Transactions involving high-risk transit jurisdictions - Payments routed through jurisdictions that are not directly sanctioned but are commonly used as intermediaries to facilitate transactions with sanctioned countries.

- Payments involving newly-introduced counterparties - Transactions involving counterparties that were not previously associated with the relationship or that are inconsistent with the client's known business activities or geographic footprint.

- Transactions involving counterparties with limited economic presence - Payments involving entities that appear to have minimal operational presence, no clear business activity, or which have characteristics consistent with shell or front companies.

- Transactions involving unusually-complex payment chains - Payments involving multiple intermediaries, nested payment arrangements, or routing through multiple jurisdictions without an apparent commercial rationale.

- Sudden changes in transaction behaviour - Significant increases in transaction volume, value, or frequency that are inconsistent with the expected activity of the client or with the client's stated business purpose.

- Payments involving high-risk sectors or sanctioned goods - Transactions where payment references, invoices, or supporting documentation indicate the potential involvement of goods, services, or sectors subject to trade restrictions, such as arms, dual-use goods, energy-related equipment, aviation components, or other restricted items.

- Transactions involving vessels or aircraft subject to restrictions - Payments relating to vessels or aircraft that are subject to sanctions measures, or where shipping or aviation information indicates possible links to sanctioned entities.

- Transactions involving sanctioned ports or shipping routes - Payments linked to shipping routes, ports, or maritime services associated with sanctioned jurisdictions or sanctioned maritime operators.

- Payments referencing restricted projects or sectors - Transactions linked to sectors that are subject to sectoral sanctions, such as defence, military equipment, certain energy projects, or specified industrial sectors.

- Transactions structured to obscure the involvement of a designated person - Transactions where payments are made to entities that appear to act as intermediaries or pass through vehicles without a clear commercial role.

- Transactions involving ownership or control indicators - Payments involving entities whose ownership or control structure suggests a potential connection to a designated person, particularly where ownership chains involve jurisdictions or entities associated with sanctions evasion.

- Rapid movement of funds between related parties - Transactions where funds are quickly transferred between multiple entities within a short period of time in a manner that may indicate attempts to obscure the ultimate beneficiary.

- Use of newly-established or dormant entities - Transactions involving entities that have been recently incorporated or that have limited transaction history but suddenly begin conducting high value transactions.

- Transactions involving repeated payment reversals or re-routing - Payments that are repeatedly rejected, re-routed, or re submitted with modified beneficiary details or payment references.

Operators should also consider the use of network or relationship analysis as part of their transaction monitoring arrangements. Network analysis can assist in identifying indirect links between clients, counterparties, and other entities that may indicate the involvement of designated persons or coordinated attempts to circumvent sanctions. For example, network analysis may reveal patterns such as multiple clients transacting with the same high-risk counterparty, clusters of entities linked through common directors or ownership, or repeated use of the same intermediary entities across different client relationships.

This is particularly valuable in the context of sanctions compliance because designated persons frequently seek to distance themselves from transactions through layered ownership structures, intermediaries, or networks of related entities in order to conceal their involvement.

Transaction monitoring rules and scenarios should be reviewed periodically to ensure that they remain effective and aligned with the Operator's sanctions risk profile, and effective in identifying potential sanctions exposure.

4.11.4 Reviewing the Customer Risk Rating

The CRA should not be treated as a one-off exercise. Operators should review the client's risk rating periodically and also whenever new information becomes available that may affect the sanctions risk associated with the relationship.

This may include situations where:

- New parties become involved in the relationship or transaction;
- Changes occur in the client's ownership or control structure;
- Adverse media or other relevant information is identified; or
- Monitoring activities indicate an increased risk of sanctions exposure.

Where the risk level associated with a client changes, Operators should ensure that the monitoring and control measures applied to the relationship are adjusted accordingly.

4.12 Understanding the Context and Objective of the Relationship or Transaction

While the preceding sections have focused primarily on identifying the parties associated with a relationship or transaction and screening those parties against applicable sanctions lists, Operators should recognise that effective sanctions due diligence also requires an understanding of the context and objective of the relationship or transaction.

Sanctions exposure does not arise only from the identity of the parties involved. It may also arise from the nature of the activity being undertaken, the jurisdictions connected to it, the sectors involved, or the economic purpose of the transaction.

For this reason, Operators should ensure that they understand the nature and purpose of the relationship or transaction and assess whether it is consistent with the client's profile, business activities and expected transaction behaviour. This understanding should inform multiple stages of the Sanctions CDD process. In particular, it is relevant when:

- Identifying the parties that may be associated with a relationship or transaction;
- Determining which parties should be screened;
- Assessing the sanctions risk associated with a client through the CRA;
- Reviewing transactions as part of ongoing monitoring; and
- Identifying indicators that a structure or transaction may be designed to conceal the involvement of a designated person or to circumvent restrictive measures.

Operators should therefore ensure that information obtained regarding the context and objective of the relationship or transaction is considered throughout the Sanctions CDD process and reflected in the Operator's assessment of sanctions exposure.

Where the context or objective of the relationship or transaction cannot be clearly understood, this may indicate an elevated risk that the structure is intended to conceal the involvement of a designated person or to circumvent restrictive measures.

EXAMPLE 1 – Unclear purpose of a relationship

A newly incorporated trading company seeks to establish a relationship with an Operator in order to conduct international payments. The client states that it will engage in "general trading activity" but is unable to explain the nature of the goods involved, the jurisdictions with which it intends to trade, or the counterparties it expects to deal with. The ownership structure includes multiple intermediate entities, and the client provides inconsistent explanations regarding the role of an intermediary involved in arranging transactions.

In this situation, the Operator is unable to form a clear understanding of the commercial purpose of the relationship or the nature of the transactions that will be conducted. This lack of clarity may indicate that the structure could be used to obscure the involvement of another party or to facilitate transactions that may give rise to sanctions exposure. The Operator should therefore conduct further enquiries and should not proceed with establishing the relationship until the purpose of the relationship can be clearly understood.

EXAMPLE 2 – Unclear purpose of a relationship

MedSupply Trading Ltd, a Malta-incorporated company approaches the Operator to establish a business relationship in order to process payments relating to the import and resale of medical equipment within the EU. During onboarding, the client states that:

- It sources medical devices from manufacturers in Asia;
- It sells these products to hospitals and distributors within the EU; and
- Payments processed through the Operator will relate to these activities.

The ownership structure of MedSupply Trading Ltd is straightforward. The Operator identifies and screens: the client; its beneficial owner, Mr A; and its directors. No sanctions concerns are identified at this stage.

Shortly after onboarding, the Operator observes the following pattern:

- MedSupply Trading Ltd requests the Operator to process a series of payments to Caspian Logistics LLC, a company incorporated in a non-EU jurisdiction not subject to comprehensive sanctions;

- The payments are described as relating to "logistics support" and "distribution services";

- The value of these payments is significant and represents a large proportion of the client's transaction volume;

- Shipping documentation provided indicates that goods are routed through multiple intermediary jurisdictions before reaching their stated destination; and

- The end destination of certain shipments appears to be a jurisdiction subject to EU restrictive measures on specific categories of goods.

The Operator screens Caspian Logistics LLC and no sanctions concerns are identified. Defined the lack of concerns arising via screening, sanction risk arises in this from the nature and purpose of the transaction.

In circumstances such as those described above, the Operator should not rely solely on the fact that the parties have been identified and screened. Instead, the Operator should take steps to understand whether the transaction is lawful in substance.

The Operator should request sufficient information to understand:

- The commercial purpose of the transaction;

- The role of each party involved, including Caspian Logistics LLC;

- The origin and destination of the goods; and

- The economic rationale for the routing of funds and goods through multiple jurisdictions.

The explanation provided should be consistent, plausible and aligned with the client's stated business activities.

The Operator should obtain documentation sufficient to verify the explanation provided. This may include:

- Contracts or commercial agreements;
- Invoices and purchase orders;
- Shipping and transport documentation (including bills of lading);
- Customs documentation; and
- Information on the end customer or end destination.

On the basis of the information obtained, the Operator should assess whether the transaction may:

- Involve a sanctioned jurisdiction, directly or indirectly;
- Relate to goods, services or sectors subject to restrictive measures; or
- Be structured in a way that conceals the true destination or end-user.

This assessment should focus on the substance of the transaction, not only its formal structure.

The Operator should make a determination as to whether it can satisfy itself that:

- The transaction does not result in funds or economic resources being made available, directly or indirectly, to a designated person; and
- The transaction does not breach, or seek to circumvent, applicable restrictive measures.

Where the Operator is able to satisfy itself that the transaction is lawful, it may proceed, subject to appropriate monitoring.

Where the Operator is unable to obtain sufficient clarity, or where concerns remain as to the true nature or destination of the transaction, the Operator should not process the transaction.

The Operator should assess whether the documentation supports the stated purpose of the transaction and whether there are inconsistencies or gaps.

Where the Operator is unable to obtain sufficient information to understand the context or objective of the relationship or transaction, the Operator should take reasonable steps to clarify the situation. This may include requesting additional information or documentation from the client or seeking information from independent or reliable sources.

If, after taking reasonable steps, the Operator remains unable to form a clear understanding of the purpose of the relationship or transaction, the Operator should not proceed with establishing the business relationship or executing the transaction.

The Operator should also consider whether the inability or unwillingness of the client to provide a clear explanation may indicate an elevated risk that the structure or transaction is intended to conceal the involvement of a designated person or to circumvent restrictive measures. Where such suspicion arises, the Operator should consider whether a report to the competent authority may be appropriate in accordance with its reporting obligations.

Important

Sanctions due diligence is not a question of comfort but of legality. Operators must satisfy themselves that a relationship or transaction does not result in a breach of applicable restrictive measures. Where this cannot be established, the Operator should decline to proceed or consider seeking professional advice.

4.13 Governance of Sanctions CDD

Clear ownership - Operators should ensure that clear responsibility is assigned for the preparation, maintenance and oversight of each of the components of Sanctions CDD described above.

Senior management approval - Each of the components of Sanctions CDD should be reviewed and approved at an appropriate level of senior management.

Integration with the control framework and decision-making - Each of the components of Sanctions CDD should be treated as an active component of the Operator's Sanctions Framework rather than as a purely formal control and should be fully and effectively integrated within it.

For additional information please see Section 12.

4.14 Documentation

Operators should ensure that all components of Sanctions CDD are clearly documented.

The documentation should describe the methodologies and, where applicable, the risk factors considered, the conclusions reached and the mitigating measures implemented to address the risks identified. The documentation should describe how sanctions risk relating to prospective and existing clients is identified, managed and mitigated.

Documentation relating to all Sanctions CDD components should be maintained in a form that can be made available to the SMB upon request.

Operators should also ensure that documentation is updated when material changes occur in the Operator's activities, risk profile or control environment.

For additional information please see Section 8.

BORD TA' SORVELJANZA DWAR IS-SANZJONIJIET
SANCTIONS MONITORING BOARD
MALTA

Chapter 5

Freezing and Reporting Controls

5. Freezing and Reporting Controls

Under Article 31(1) of the NIA, the publication of sanctions measures by the UN Security Council, the EU, or through the imposition of a freezing measure by national regulations, has the force of law in Malta and is equivalent to a freezing order.

As a result, where a situation is identified that constitutes, or may constitute, a breach of sanctions, whether directly or indirectly, the relevant transaction must not proceed. Any funds or economic resources involved must be frozen without delay, and the SMB must be notified in accordance with the applicable reporting procedures.

In practice, this means that Operators should have procedures in place to:

- Review and verify potential matches identified through sanctions screening or other controls;
- Take immediate steps to freeze relevant funds or economic resources where a match with a designated person, entity, or body is confirmed;
- Report confirmed matches to the SMB without delay;
- Report frozen funds and economic resources to the SMB in accordance with the applicable reporting requirements;
- Ensure that frozen funds and economic resources remain subject to effective restrictions and are monitored on an ongoing basis; and
- Report to the SMB situations where they know, suspect, or have reasonable grounds to suspect, that sanctions may have been breached or circumvented, even where no designated person has been identified.

The following sections set out the obligations relating to the freezing of assets and the reporting of sanctions hits and suspected breaches.

5.1 Reviewing and Verifying Potential Matches

Where a potential match is identified through sanctions screening or other monitoring processes, Operators should promptly verify whether the person or entity corresponds to a designated person.

This verification should involve comparing the available identifying information relating to the client, counterparty, or other relevant party with the information contained in the relevant sanctions listing. Operators should take reasonable steps to determine whether the match is a true match or a false positive.

Operators should have procedures in place to ensure that potential matches and suspected breaches are promptly escalated to the appropriate compliance or senior management function for review and decision.

5.2 Freezing of Funds or Economic Resources

Freezing measures under UN Security Council Resolutions and EU sanctions become effective and binding on all persons immediately upon publication and remain in force until revoked. In the case of national sanctions, freezing measures apply until the relevant delisting decision is adopted by the competent authority.

Where a match with a designated person, entity or body is confirmed, Operators must freeze the relevant funds or economic resources without delay and prevent the execution of any related transactions.

In accordance with Article 31 of the NIA, all funds and economic resources belonging to, owned, held or controlled, directly or indirectly, by a designated person, entity or body, must be frozen without delay and without prior notice.

The freezing obligation also extends to entities that are owned or controlled, directly or indirectly, by a designated person. Operators should therefore consider whether a designated person holds a majority ownership interest or otherwise exercises control over an entity.

This obligation also extends to:

- assets derived from such funds or economic resources; and
- assets held by persons or entities acting on behalf of, or at the direction of, a designated person or entity.

It is also prohibited to make funds, economic resources, property, or financial or related services available, directly or indirectly, to or for the benefit of a designated person or a related entity, unless expressly authorised under the applicable sanctions regime.

For the purposes of determining the scope of assets and actions subject to sanctions-related restrictions, Operators should apply the following NIA definitions:

- Freezing of funds refers to the prevention of any movement, transfer, alteration, use of, access to, or dealing with funds in a manner that would result in any change to their volume, amount, location, ownership, possession or character.

- Freezing of economic resources refers to preventing the use of such resources to obtain funds, goods or services by any means, including through sale, hire or encumbrance.

- Funds include financial assets and benefits of every kind, including cash, deposits, securities, debt instruments, interest and dividends, credit facilities, trade finance instruments, documentary evidence of financial interests, and crypto-assets as defined under applicable EU legislation.

<u>Frequent challenges</u> - Operators frequently struggle with operationalising the freezing obligation, rather than understanding the legal rule itself. In practice, difficulties often arise in the areas below.

- *Identifying assets beyond the primary account* - Operators may freeze the most visible asset, such as a bank account, but fail to identify other funds or economic resources belonging to or controlled by the designated person. These may include securities accounts, trade finance instruments, crypto-asset wallets, collateral or pledged assets, and assets held through subsidiaries or special purpose vehicles.

- *Ownership and control analysis* - A frequent difficulty arises where the designated person does not appear as the direct account holder. Operators may fail to identify entities that are owned or controlled by a designated person, particularly where ownership is layered across multiple jurisdictions or where control is exercised informally.

- *Indirect provision of funds or economic resources* - Operators often focus on freezing existing funds but overlook the separate prohibition on making funds or economic resources available, directly or indirectly, to a designated person. Examples may include making payments to an entity acting on behalf of a designated person, providing goods or services to a designated person through an intermediary, or continuing to perform contractual services that generate financial benefit for a designated person.

- *Freezing economic resources rather than funds* - Operators generally understand the freezing of monetary assets but may struggle with the concept of economic resources. These may include assets such as real estate, vehicles, machinery, vessels or aircraft, and intellectual property. Ensuring that such assets cannot be used to obtain funds, goods or services may require additional operational controls.

- *Maintaining the effectiveness of the freeze* - Another challenge is ensuring that the freeze remains effective over time. Operators may fail to ensure that additional funds credited to a frozen account are also frozen, that interest, dividends or other proceeds remain frozen, or that internal systems prevent any form of access to or movement of frozen assets.

- *Coordination across internal systems* - Freezing obligations often require coordination across different operational systems, such as payments processing, custody platforms, trade finance systems, and treasury systems. Where systems are not properly aligned, a freeze applied in one system may not prevent activity in another.

- *Speed of implementation* - Sanctions freezes must be applied without delay. In practice, however, internal approval processes or manual intervention may slow implementation, creating a risk that transactions may proceed before the freeze is effectively applied.

Operators should be aware of these typical operational challenges and ensure that their policies, procedures, and systems are capable of identifying all relevant assets, assessing ownership and control relationships, and implementing freezing measures promptly and effectively across all relevant business lines.

Confirmed matches with national sanctions issued by other states

Where a person, entity, or body is designated under the sanctions regime of a third country, Operators are expected to assess the reasons for the designation and to consider the transaction or relationship in light of those reasons, any connection to Malta, and any applicable legal or regulatory obligations, including those arising under AML/CFT legislation.

Any hits identified in relation to individuals or entities listed under national sanctions regimes of other states may be voluntarily reported to the SMB, in accordance with the applicable reporting procedures.

Authorisation request

In certain circumstances, the applicable sanctions regime may permit the release of frozen funds or the making available of funds or economic resources under an authorisation issued by the SMB in Malta or where jurisdiction lies elsewhere, by the competent authority of another Member States.

Operators must not release or otherwise deal with frozen funds or economic resources unless a valid authorisation has been issued by the SMB or the competent authority responsible for the relevant sanctions regime.

5.3 Reporting Confirmed Matches to the SMB

Where a match with a designated person, entity, or body has been confirmed, Operators must report the sanctions hit to the SMB without delay. Reports must be submitted using the standard reporting template made available on the SMB website and must be transmitted electronically in accordance with the instructions issued by the SMB. Reports submitted to the SMB should be complete and accurate. Operators should include all relevant information available to them, including identifying information relating to the designated person, and details of the relationship or transaction concerned.

Supporting documentation should be provided where available. This may include identification records, account information, transaction records, or other documents relevant to the sanctions hit.

Incomplete submissions may be returned by the SMB for further clarification or additional information.

5.4 Reporting Frozen Funds and Economic Resources to the SMB

Where funds or economic resources have been frozen in accordance with the applicable sanctions regime, Operators are required to report such assets to the SMB without delay upon identification of the targeted property.

In addition to this initial notification, Operators are required to submit reports on frozen assets on an annual basis, in accordance with the reporting requirements

established by the SMB. This requirement applies where there are fluctuations in the frozen funds accounts, including, for example, the accrual of interest or dividends, or where authorised payments have been made.
Reports submitted to the SMB should include, where available, information relating to:

- The nature and value of the frozen funds or economic resources;
- The date on which the assets were identified and frozen;
- The manner in which the assets are held;
- Relevant account or asset details; and
- Any other information relevant to the implementation of the freezing measure.

Reports must be completed using the prescribed reporting template and submitted in accordance with the instructions issued by the SMB. Supporting documentation should be provided where available.

Operators should ensure that accurate records are maintained in relation to frozen funds and economic resources, including the steps taken to implement the freeze and the information reported to the SMB. This will assist Operators in meeting their ongoing reporting obligations and in ensuring that the freezing measures remain effective for as long as the designation remains in force.

In cases where the Operator is:

A. acquiring customers from other companies where frozen funds and/or economic resources are involved;
B. transferring customers between companies where frozen funds and/or economic resources are present; or
C. closing a business or company involving customers with frozen funds and/or economic resources,

the SMB should be informed immediately so that appropriate guidance can be provided on the necessary steps to be taken.

5.5 Ongoing Monitoring of Frozen Assets

Operators must ensure that the freezing of funds or economic resources remains effective for as long as the relevant designation remains in force.

In practice, this requires Operators to ensure that frozen assets cannot be accessed, moved, transferred, or otherwise used in any way that would alter their value, ownership, or availability. Operators should also ensure that any additional funds credited to frozen accounts, including interest, dividends, or other proceeds, are accrued in a separate frozen account and not made available, directly or indirectly, to the designated person. Also, any issuance of payments from the frozen accounts requires an authorization from the SMB.

Operators should maintain appropriate controls to ensure that frozen assets remain identified within their systems and that no transactions or actions affecting those assets can be executed without appropriate review and authorisation.

Where relevant, Operators should also ensure that frozen assets remain subject to ongoing monitoring in order to identify any attempted transactions, changes in ownership or control structures, or other developments that may affect the implementation of the freezing measures.

5.6 Reporting of Suspected Violations

In addition to reporting confirmed sanctions hits, Operators are required to notify the SMB where they know, suspect, or have reasonable grounds to suspect that sanctions may have been breached or circumvented by the client or a third party

In accordance with Article 32(1)(e) of the NIA, this obligation applies in relation to breaches or attempted circumvention of restrictive measures adopted by the UN Security Council, EU, or under Maltese law.

This reporting obligation applies regardless of whether:

- Funds or economic resources are involved;
- A designated person has been identified; or
- The transaction has been completed.

It also applies to attempted or unsuccessful transactions, including situations where a transaction is halted or rejected after concerns relating to sanctions arise.

In practice, Operators should consider reporting to the SMB where a transaction, relationship, or activity gives rise to concerns that sanctions may be breached or circumvented. Examples may include situations where:

- A client attempts to restructure or reroute a transaction after a sanctions alert is raised;
- Transactions appear to involve intermediaries or entities that may be acting on behalf of a designated person;
- Payments are routed through multiple jurisdictions or intermediaries without a clear commercial rationale;
- Documentation, payment references, or transaction details suggest the possible involvement of sanctioned goods, sectors, vessels, aircraft, or jurisdictions;
- Counterparties appear to have been introduced to obscure the identity of the ultimate beneficiary of funds or economic resources; or
- A client attempts to proceed with a transaction after being informed that sanctions concerns have been identified.

For the purposes of this obligation the following definitions apply:

- *Knowledge* - Knowledge refers to situations where an Operator or its employees are aware, based on information or evidence available to them, that a breach of sanctions or an attempt to circumvent sanctions has occurred, is occurring, or may occur;
- *Suspicion* - Suspicion arises where objective facts or circumstances give rise to concern that sanctions may have been breached or circumvented, even where conclusive evidence is not available; and
- *Reasonable grounds to suspect* - Reasonable grounds to suspect exist where a reasonable person, having regard to the available facts and circumstances, would conclude that a breach or circumvention of sanctions may be taking place.

Where such situations arise, Operators should ensure that the matter is promptly escalated internally to the appropriate compliance or senior management function

for assessment. Where the threshold of knowledge, suspicion, or reasonable grounds to suspect is met, the matter should be reported to the SMB without delay in accordance with the applicable reporting procedures.

EXAMPLE – A scenario that might require reporting even where no designated person has been identified.

An Operator processes payments for a client involved in the trading of industrial equipment. The client submits payment instructions to a newly introduced company incorporated in Country B.

During the transaction review, the Operator notes that the invoice and accompanying shipping documentation indicate that the equipment will be delivered to a company located in a jurisdiction subject to EU sanctions affecting certain industrial sectors.

The Operator requests further clarification from the client regarding the destination of the goods and the role of the intermediary company. In response, the client withdraws the payment instruction and submits a revised instruction requesting that the funds instead be transferred to a different intermediary company located in another jurisdiction. The client provides limited information regarding the ultimate destination of the goods.

Although no designated person has been identified through sanctions screening, the available information and the client's attempt to restructure the transaction, raise concerns that the transaction may be intended to circumvent restrictive measures.

In these circumstances, the Operator should not proceed with the transaction and should report the matter to the SMB as a suspected attempt to circumvent sanctions.

Where transactions are rejected due to sanctions prohibitions, such cases should be reported through a Suspicion of Violations report.

5.7 Additional Reporting Obligations under Applicable Sanctions Regimes

Restrictive measures adopted by the EU and the UN Security Council, as well as relevant national measures, are published on the website of the SMB. Operators are expected to remain informed of updates to applicable sanctions regimes and to comply with any reporting obligations specific to the relevant regime, as these may differ depending on the legal framework under which the designation is made. Operators are also subject to additional reporting obligations set out in other guidance documents issued by the SMB.

5.8 Governance of Freezing and Reporting Controls

Clear ownership - Operators should ensure that clear responsibility is assigned for the implementation and oversight of the freezing and reporting controls described in this chapter. This should include responsibility for reviewing sanctions hits, confirming matches, implementing freezing measures, and ensuring that reporting obligations to the SMB are fulfilled without delay.

Senior management oversight - Operators should ensure that appropriate oversight arrangements are in place to monitor the effectiveness of controls relating to the freezing of funds and economic resources and the reporting of sanctions hits and suspected violations. Senior management should ensure that sufficient resources, systems, and procedures are in place to enable Operators to comply with these obligations.

Integration with the control framework and decision-making - The processes for identifying sanctions matches and circumvention attempts, freezing assets, and reporting to the SMB should be fully and effectively integrated into the Operator's broader Sanctions Framework. Operators should ensure that these processes are treated as active operational controls and that relevant staff are able to identify, escalate, and respond to sanctions-related events promptly.

For additional information please see Section 8.

5.9 Documentation

Operators should ensure that the actions taken in relation to sanctions hits, the freezing of funds or economic resources, and the reporting of suspected breaches are appropriately documented.

This documentation should include where applicable:

- The information used to verify potential matches;
- The basis on which a sanctions hit was confirmed or rejected;
- Details of the funds or economic resources froze;
- The actions taken to implement the freezing measures; and
- The reports submitted to the SMB.

Documentation should be maintained in a form that can be made available to the SMB upon request. Operators should also ensure that records relating to sanctions hits, frozen assets, and reports submitted to the SMB are retained for an appropriate period and are accessible for review where required.

For additional information please see Section 12.

BORD TA' SORVELJANZA DWAR IS-SANZJONIJIET
SANCTIONS MONITORING BOARD
MALTA

Chapter 6
Tipping-off Controls

6. Tipping off Controls

Operators are prohibited from informing clients or any third parties in advance that a freezing measure is to be applied.

This obligation, set out in Article 32(8) of the NIA, is intended to prevent the circumvention of restrictive measures by ensuring that freezing actions cannot be avoided once they are initiated. Operators should therefore ensure that their Sanctions Framework includes appropriate measures to prevent such disclosures.

In practice, for Operators this means:

- Restricting knowledge of a pending or imminent freezing measure strictly to those persons who require the information in order to implement the measure;

- Ensuring that internal procedures clearly prohibit employees from informing the client, or any other third party, that a freezing action is being considered or is about to be applied;

- Implementing internal escalation procedures so that potential freezing measures are assessed and authorised by the appropriate senior personnel before any operational steps are taken;

- Ensuring that communications with the client or other parties during the period in which a freezing measure is being assessed are carefully managed so that they do not inadvertently signal that a freeze may occur;

- Limiting internal circulation of information relating to freezing measures, including through appropriate access controls, confidentiality obligations and secure handling of documentation; and

- Ensuring that staff involved in onboarding, account management, payments processing and compliance functions receive appropriate training on the prohibition against advance disclosure and the importance of maintaining confidentiality in sanctions matters.

6.1 Restricting Access to Sensitive Sanctions Information

Access to information relating to potential or pending freezing measures should be limited to personnel who require it for the performance of their duties. Access should be controlled on a need-to-know basis and staff should understand the sensitivity of such information.

6.2 Prohibition on Advance Disclosure

Operators should establish clear internal rules prohibiting employees from informing the client or any third party that a freezing measure is being considered or is about to be applied. This prohibition should apply whether the disclosure would be made intentionally or inadvertently, including through informal conversations, client communications or explanations relating to delays or restrictions in the processing of transactions.

6.3 Internal Escalation and Authorisation

Operators should implement internal escalation procedures for situations where a potential freezing measure may be required. These procedures should ensure that relevant information is promptly referred to the compliance function or other designated personnel responsible for sanctions compliance. Where appropriate, the decision to apply a freezing measure should be reviewed or authorised at a sufficiently senior level within the organisation, in accordance with the Operator's governance framework. Clear escalation channels help ensure that freezing measures are applied consistently and that decisions are taken by individuals with the appropriate expertise and authority.

6.4 Management of Client Communications

Where a potential freezing measure is being assessed, Operators should manage communications with the client and other parties with particular care to avoid inadvertently signalling that a freezing action may occur. The prohibition of tipping-off does not prevent the Operator from requesting or verifying the information necessary to fulfil CDD or EDD obligations. However, these interactions must be conducted carefully and without disclosing, either explicitly or implicitly, that sanctions concerns or freezing measures are under consideration.

In situations where suspicion exists, but certainty has not yet been established. In such cases, Operators are expected to handle communications cautiously until sufficient certainty is obtained and the freezing measures could be applied.

6.5 Controlled Internal Handling of Information

Operators should ensure that information relating to freezing measures is handled with appropriate confidentiality controls. This may include restricting access to relevant files and systems, ensuring that documentation relating to potential freezing measures is stored securely, and limiting the circulation of internal communications discussing the matter. Appropriate access controls help ensure that sensitive information does not reach individuals who are not involved in the sanctions assessment or implementation process.

6.6 Training and Staff Awareness

Staff should receive training on the prohibition against informing clients or third parties in advance of a freezing measure. Training should explain the legal basis for the prohibition, the risks associated with advance disclosure, and the practical situations in which the issue may arise. Particular attention should be given to staff in compliance, onboarding, payments processing and client-facing roles, as these individuals may encounter circumstances in which sanctions concerns arise. Regular training and awareness programmes help ensure that staff understand both the importance of confidentiality and the consequences of breaching this obligation. Refer to Section 10 on more information about Training.

6.7 Governance of Tipping Off Controls

Clear ownership - Operators should ensure that clear responsibility is assigned for the implementation and oversight of the controls designed to prevent the advance disclosure of freezing measures or sanctions related reporting.

This should include responsibility for ensuring that information relating to sanctions assessments, potential freezing measures and reporting obligations is handled with appropriate confidentiality, and that internal procedures effectively prevent the client or other third parties from being informed in advance that a freezing measures are to be applied.

Senior management oversight - Operators should ensure that appropriate oversight arrangements are in place to monitor the effectiveness of controls designed to prevent the advance disclosure of freezing measures and other sanctions-related actions.

Senior management should ensure that sufficient governance arrangements, procedures and staff training are in place to ensure that sanctions-related information is handled with an appropriate level of confidentiality and that employees understand the prohibition against advance disclosure.

Integration with the control framework and decision-making - Controls designed to prevent advance disclosure should be fully and effectively integrated into the Operator's broader Sanctions Framework.

In particular, procedures relating to sanctions screening, the assessment of potential matches, the implementation of freezing measures and the submission of reports to the SMB should incorporate safeguards to ensure that these processes are conducted confidentially and do not result in the client or other parties being alerted to the application of restrictive measures.

For additional information please see Section 8.

BORD TA' SORVELJANZA DWAR IS-SANZJONIJIET
SANCTIONS MONITORING BOARD
MALTA

Chapter 7
Policies and Procedures

7. Policies and Procedures

Operators must establish and maintain:

a. Policies describing the standards they apply to comply with their obligations under the NIA; and

b. Procedures describing the procedural steps and methodologies that they apply to achieve those standards.

Policies and procedures should be formally approved by senior management and reviewed periodically to ensure that they remain effective and aligned with applicable legislative and regulatory developments. Policies and procedures should cover, at a minimum:

- *SRA* - Describing the standards and procedural steps that Operators apply to assess the sanctions risk to which their businesses are exposed.

- *Sanctions CDD* – Describing the standards and procedural steps that Operators apply to performing each of the components of Sanctions CDD (including specifying the categories of parties subject to sanctions screening, the timing of such screening, the actions taken to discount potential screening matches and the approach to ongoing monitoring).

- *Freezing and reporting controls* – Describing the standards and procedural steps that Operators apply when a confirmed match with a designated person is identified, including procedures for escalation, verification of the match, the immediate freezing of funds or economic resources where required, and the submission of reports to the competent authority in accordance with applicable legal obligations.

- *Tipping -off controls* – Describing the standards and procedural steps that Operators apply to ensure that they prevent the disclosure of information that could prejudice sanctions compliance measures or investigations, including restrictions on communications with affected persons and guidance to staff on the handling of such situations.

It is important that policies and procedures be clear and unambiguous so as to enable their correct and consistent application. They should be tailored to the specific activities, risk profile and operating model of the Operator, rather than reproducing regulatory provisions without adaptation. Policies and procedures should also, where relevant:

- Identify the applicable legislation from which sanctions obligations arise and specify the sanctions regimes relevant to the Operator’s activities;
- Describe the legal, regulatory and disciplinary consequences of non-compliance with sanctions obligations;
- Establish clear escalation and decision-making protocols;
- Describe the process for seeking - guidance from competent authorities where uncertainty arises;
- Establish internal reporting and whistleblowing channels to enable staff to report potential breaches, concerns or weaknesses in sanctions controls;
- Describe the procedures for requesting derogations, licences or guidance from the SMB where applicable;
- Specify sanctions training requirements, including frequency, target audience and record-keeping requirements; and
- Define document and record retention requirements in line with applicable legal and regulatory obligations.

Policies should be formally documented, communicated to relevant staff and periodically reviewed to ensure that sanctions controls are applied consistently and remain effective in practice.

BORD TA' SORVELJANZA DWAR IS-SANZJONIJIET
SANCTIONS MONITORING BOARD
MALTA

Chapter 8
Record-Keeping

8. Record-keeping

Operators should maintain appropriate records relating to the operation of their Sanctions Framework. Effective record-keeping supports transparency, facilitates internal oversight and provides evidence that the Operator has applied sanctions controls in accordance with applicable legal and regulatory requirements.

Records should be sufficiently detailed to enable the Operator and competent authorities to understand the basis on which sanctions-related decisions were taken and to verify that appropriate procedures have been followed. These records must be made available to the SMB or other supervisory authorities upon request.

In particular, Operators should ensure that records are maintained in relation to:

- SRA and any updates or revisions made to them;
- Sanctions policies, procedures and internal guidance;
- Sanctions CDD conducted both at onboarding and on an ongoing basis. These records (collectively known as "Verification Records"), are critical and Operators should ensure that the rationale supporting the acceptance of a client, particularly in cases where information or documentation is incomplete, unclear, or presents elevated risk factors, is properly recorded and retained. This rationale should demonstrate that the decision was made following a thorough risk-based assessment and appropriate internal escalation or approval procedures. Such scenarios may include, but are not limited to, the acceptance of a client despite obfuscation of ownership or control; complex or layered corporate structures; involvement in, or connection to, high-risk jurisdictions known for or have potential for sanctions evasion; or lack of cooperation or transparency from the client during the verification process.

Where such high-risk decisions are made, Operators should document the mitigating measures applied, the senior management approval obtained (if applicable), and any enhanced due diligence performed to justify and support the decision. These records serve to demonstrate that a considered and proportionate approach was taken in line with the SRA, risk appetite and compliance obligations.

Where documents have been certified or attested by an authorised person as part of the verification process, the certification copies and related correspondence must also be retained as they serve as proof of authenticity and support the traceability of the verification process;

- Sanctions screening activities (both manual and automated), including alerts generated and the outcome of reviews conducted (collectively known as "Screening Records"). Operators should ensure that the rationale for screening results, risk-assessment and other decisions made based on those results, are properly documented;

- The parameters and rules applied to their transaction monitoring to identify indicators of potential sanctions breaches;

- The freezing of funds or economic resources and any reports submitted to the competent authority;

- Internal escalations and decisions relating to sanctions matters;

- Sanctions-related management information provided to senior management, along with minutes of discussions at relevant committees;

- Information relating to the ongoing review of the Sanctions Framework (including in the form of Compliance assurance, Internal Audit testing, effectiveness reviews and other periodic reviews) along with results and details of remedial actions required and taken; and

- Training provided to staff in relation to sanctions compliance.

Where an automated screening system does not provide an audit trail of each screening performed but instead records only the initial registration date and generates alerts where potential matches are identified, the system will only be considered compliant if sanctions screening is conducted on a daily basis. Operators should maintain evidence, including contractual documentation with the service provider where applicable, explicitly confirming that sanctions screening is conducted on a daily basis

8.1 Retention Period

Operators must retain compliance records for a minimum period of five (5) years. This period commences from the specific dates prescribed in law, depending on the nature of the records being held.

The retention period begins:

- From the date when the Operator no longer provides services to the client, in the case of Verification Records and other records demonstrating compliance with identification and verification obligations at Article 32 (a) of the NIA.

- From the date on which a particular compliance check or screening takes place, in the case of Screening Records or records of other ongoing or event-based monitoring activities undertaken to comply with obligations at Article 32 (b) of the NIA; and

- From the date when the Operator ceases to fall within the categories listed in Schedule I, in relation to any other records created to comply with any other obligation arising from the NIA.

8.2 Extension of Retention Period

In accordance with the proviso under Article 32(9) of the NIA, the SMB may extend the standard five-year retention period where it is deemed strictly necessary for the purpose for which the information is processed. The need for such extensions may arise, for example, where records are required in connection with investigations, enforcement action or ongoing legal or regulatory proceedings.

Operators must comply with any such directive and ensure that records continue to be retained securely for the extended period specified by the SMB.

Where an extension is applied, Operators should document the basis for the extension and period for which the records are to be retained. During this time, records should continue to be protected against unauthorised access, alteration, or destruction. Once the extended period has expired and the information is no longer required, records should be disposed of securely in accordance with applicable data protection and confidentiality requirements.

8.3 Data Protection, Information Handling and Record Retention

Operators will process personal data when implementing their Sanctions Framework within the meaning of article 4(1) of the General Data Protection (the "GDPR"). This may include personal data relating to clients, beneficial owners, controllers, directors, authorised representatives, counterparties, intermediaries, agents, persons connected to transactions and persons identified through screening, monitoring, adverse media review, internal escalation or reporting processes. The processing of personal data for sanctions compliance purposes should be carried out in accordance with the provisions of the GDPR and the Data Protection Act (Cap. 586 of the Laws of Malta), including the regulations made thereunder.

Lawful basis and purpose of processing

Operators should identify and document the lawful basis on which personal data is processed for sanctions compliance purposes in terms of the principle of accountability as set forth in article 5(2) of the GDPR. In many cases, the processing of personal data for sanctions compliance purposes will be connected to the Operator's need to comply with legal obligations under the NIA and applicable restrictive measures in terms of article 6(1)(c) of the GDPR. Operators should, however, assess the lawful basis for processing having regard to their own activities, and the specific purpose for which the information is processed.

Operators should ensure that personal data collected for sanctions compliance purposes is used only for specified, explicit and legitimate purposes. These may include:

- Identifying and verifying clients and relevant parties;
- Identifying beneficial owners and persons exercising control;
- Conducting sanctions screening;
- Reviewing and resolving potential matches;
- Performing the CRA and, where required, EDD;
- Conducting adverse media checks and ongoing monitoring

- Assessing whether funds or economic resources may be made available, directly or indirectly, to a designated person or to an entity owned or controlled by one;

- Freezing funds or economic resources where required;

- Making reports to the SMB or to any other competent authority where required by law;

- Responding to requests for information from the SMB; and

- Demonstrating compliance with obligations under the NIA.

Personal data collected for sanctions compliance purposes should not be used for unrelated purposes unless the Operator has identified a lawful basis for doing so and such further processing is compatible with the purpose for which the personal data are initially collected pursuant to the requirement set forth in article 6(4) of the GDPR.

Data minimisation - Operators should collect and process personal data that is adequate, relevant and limited to what is necessary for the performance of sanctions compliance obligations in accordance with article 5(1)(c) of the GDPR.

This does not mean that Operators should avoid collecting information that is necessary to identify sanctions exposure. Where information is required to identify a client, beneficial owner, controller, counterparty, intermediary or other relevant party, to conduct sanctions screening, or to assess ownership, control or funds flow risk, the Operator should obtain sufficient information that is necessary to perform those obligations effectively.

However, Operators should not collect personal data that is not needed for the relevant sanctions compliance purpose. For example, where a particular item of information is not necessary to distinguish a person from a potential sanctions match, to understand ownership or control, or to assess the sanctions exposure arising from the relationship or transaction, the Operator should consider whether collecting that information is proportionate.

Information handling and access controls - Operators should ensure that personal data processed for sanctions compliance purposes is handled securely and accessed only by persons who require access for legitimate sanctions compliance, operational, governance, legal or regulatory purposes.

Operators should implement appropriate information handling arrangements, including:

- Clear internal procedures governing the collection, use, storage, disclosure and deletion of sanctions compliance information;
- Access controls limiting access to Sanctions CDD, screening, monitoring, escalation, freezing and reporting records to staff with a legitimate need to access them;
- Additional restrictions on access to sensitive sanctions information, including information relating to potential or confirmed matches, suspected breaches or reports to the SMB;
- Secure channels for the transmission of information internally and externally;
- Procedures to ensure that information is not disclosed to clients or third parties in a manner that would be inconsistent with tipping off controls or with any applicable legal restriction;
- Controls over the downloading, copying, printing or onward transmission of sanctions compliance records;
- Secure arrangements for the storage of electronic and physical records; and
- Procedures for the secure disposal of records once the applicable retention period has expired and the information is no longer required.

Operators should ensure that staff involved in sanctions compliance understand the sensitivity of sanctions related information and the need to handle such information in accordance with both the NIA and applicable data protection requirements.

<u>Disclosure of information</u> - Operators may need to disclose personal data to the SMB, other competent authorities, law enforcement authorities, courts, external legal advisers, auditors, group entities, third party providers or outsourced service providers in connection with sanctions compliance.

Such disclosures should be limited to what is necessary for the relevant purpose and should be made through appropriate and secure channels. Where information is disclosed to the SMB or to another competent authority in accordance with the NIA or other applicable legal requirements, Operators should retain adequate records of the information disclosed, the date of disclosure, the recipient and the basis for disclosure.

Where information is shared with group entities, third parties or service providers, Operators should ensure that the sharing is consistent with applicable data protection requirements and with the Operator's obligations under the NIA.

Third party service providers and processors - Where a third party or outsourced service provider processes personal data on behalf of the Operator in connection with sanctions compliance, the Operator should ensure that appropriate contractual and operational arrangements are in place in terms of article 28 of the GDPR. Such arrangements should address, as appropriate:

- The nature and purpose of the processing;
- The categories of personal data processed;
- The categories of data subjects whose personal data may be processed;
- The requirement for the service provider to process personal data only on documented instructions from the Operator, unless required otherwise by applicable law;
- Confidentiality obligations applicable to persons authorised to process the data;
- Technical and organisational measures to protect the data;
- Controls over the use of sub processors;
- Assistance to the Operator in responding to data subject requests and meeting applicable data protection obligations;
- Deletion or return of personal data at the end of the arrangement, subject to applicable legal retention obligations;
- Audit, testing and oversight rights; and
- The requirement for all relevant sanctions compliance records to be made available to the Operator without delay, including where required for the purpose of responding to the SMB.

Operators should ensure that reliance or outsourcing arrangements do not impair their ability to comply with either the NIA or applicable data protection requirements.

Retention of sanctions compliance records - Operators must securely retain sanctions compliance records for the period required under the NIA.

As set out this section, Operators must retain compliance records for a minimum period of five years, calculated by reference to the nature of the record concerned.

Where the SMB extends the standard retention period in accordance with Article 32(9) of the NIA, Operators must retain the relevant records securely for the extended period specified by the SMB.

Operators should ensure that their data retention policies reflect the statutory retention requirements applicable to sanctions compliance records. Such policies should identify:

- The categories of sanctions compliance records retained;
- The applicable retention period for each category of record;
- The event from which the retention period starts to run;
- The systems or locations in which the records are held;
- The persons or functions responsible for maintaining the records;
- The circumstances in which retention may be extended; and
- The process for secure disposal once records are no longer required.

Records should not be retained indefinitely unless continued retention is required by law, by the directive of the SMB or another competent authority, or by another legitimate purpose consistent with applicable data protection requirements.

Secure Disposal - Once the applicable retention period has expired and the information is no longer required; Operators should dispose of sanctions compliance records securely and in accordance with applicable data protection and confidentiality requirements.

Secure disposal should ensure that records cannot be accessed, reconstructed or used in an unauthorised manner after deletion or destruction. Operators should maintain appropriate records of disposal where necessary to demonstrate that records have been deleted or destroyed in accordance with applicable retention requirements.

Data subject rights - Operators should have procedures for handling requests from individuals by exercising rights under applicable data protection law in relation to personal data processed for sanctions compliance purposes. When responding to such requests, Operators should consider whether any restriction, exemption or other legal limitation applies, including where disclosure of information could prejudice sanctions compliance, reveal the existence of an internal review, investigation or report, or conflict with obligations under the NIA.

Operators should ensure that such requests are assessed by appropriately trained staff and, where necessary, escalate to the Operator's data protection officer, legal function or other appropriate function before a response is provided.

Personal data breaches - Operators should maintain procedures for identifying, escalating, assessing and responding to personal data breaches involving sanctions compliance information. Such procedures should ensure that potential breaches are promptly escalated to the appropriate internal function and assessed in accordance with applicable data protection requirements.

Where a third party or outsourced service provider acting as a processor processes personal data on behalf of the Operator, the Operator should ensure that the processor is required to notify the Operator without delay of any personal data breach affecting sanctions compliance information.

Governance and documentation - Operators should ensure that data protection considerations are appropriately reflected in their Sanctions Framework. This should include, where relevant:

- Documenting the purposes and lawful basis for processing personal data for sanctions compliance purposes;
- Maintaining records of processing activities where required;
- Ensuring that policies and procedures address information handling, access controls, retention and secure disposal;
- Ensuring that staff receive appropriate training on the handling of sanctions compliance information;

- Ensuring that third party and outsourcing arrangements contain appropriate data protection provisions;

- Monitoring compliance with data protection and information handling requirements; and

- Retaining records sufficient to demonstrate that sanctions compliance information has been handled in accordance with the NIA and applicable data protection requirements.

For additional information on third party reliance and outsourcing, please see Section 9.

SMB
BORD TA' SORVELJANZA DWAR IS-SANZJONIJIET
SANCTIONS MONITORING BOARD
MALTA

Chapter 9

Third-party Reliance and Outsourcing

9. Third-party Reliance and Outsourcing

Operators may occasionally find it necessary to rely on external parties or outsource certain tasks to meet their sanctions-related obligations. Such arrangements are often made to improve efficiency, access specialist expertise, or address resource limitations. While these arrangements may assist Operators in implementing sanctions controls, they should be approached with care, as the Operator remains ultimately responsible for ensuring compliance with its obligations under the NIA.

9.1 Reliance vs Outsourcing

Third party reliance refers to situations where an Operator relies on information or checks performed by another party, based on that party's own policies and procedures. This may occur, for example, where an Operator relies on due diligence information obtained by another regulated entity within the same group (this is known as intra-group reliance) or by an intermediary involved in the business relationship. In such cases, the Operator remains responsible for ensuring that the information relied upon is adequate and that reliance is permitted under applicable legal and regulatory requirements. Such reliance is permissible only under the conditions outlined below.

Outsourcing, by contrast, refers to situations where the Operator delegates the performance of certain operational tasks to an external service provider, typically using the Operator's own policies and procedures. In the context of sanctions compliance, this may include activities such as sanctions screening, support in the review of alerts, data management or independent testing of sanctions controls.

In both cases, reliance on third parties or the outsourcing of functions does not transfer responsibility for sanctions compliance. Operators remain fully accountable for ensuring that their sanctions obligations are met and should therefore maintain appropriate oversight of any such arrangements, in line with Articles 32(3) and (4).

9.1.1 Conditions for Reliance

Where an Operator relies on information or checks performed by a third party, it should ensure that appropriate safeguards are in place to ensure that such reliance does not compromise its ability to comply with its obligations under the NIA. In particular, the Operator should ensure that:

- The third party is a reputable entity and has itself been subject to appropriate due diligence by the Operator prior to the reliance arrangement being established;

- The third party maintains policies and procedures that are consistent with the obligations arising under the NIA and are compatible with the Operator's own SRA, risk appetite and compliance standards;

- The Operator is informed of any material changes to the third party's screening systems, procedures or compliance arrangements;

- The Operator is notified without delay of any sanctions matches, suspicions or adverse information identified during the due diligence process;

- Relevant findings are communicated in a timely manner so as to enable the Operator to update its own CRA;

- All Sanctions CDD information and supporting documentation are properly maintained and meet applicable statutory record-keeping requirements;

- Sanctions CDD information and documentation are to be made available to the Operator without delay where required under Article 32(4) of the NIA;

- The third party is required to notify the operators if they themselves become subject to non-compliance measures or criminal proceedings during the engagement;

- The third party is required to undertake ongoing sanctions-related training to maintain an appropriate level of competence and awareness;

- Appropriate arrangements are in place to ensure that, if the reliance arrangement is terminated, all relevant due diligence records are transferred to the Operator; and

- The Operator is able to continue meeting its legal and regulatory obligations without disruption following the termination of the arrangement.

These conditions should be clearly documented in a formal Reliance Agreement between the Operator and the third party.

The SMB expects Reliance Agreements expressly to reflect the Operator's obligation to provide any information that may be requested by the SMB, irrespective of whether a process was performed by a third party. Operators should therefore ensure that such agreements include appropriate provisions requiring the third party to make all relevant information and documentation available without delay.

Intra-group reliance on entities outside the EU - In such cases, Operators should recognise that the sanctions frameworks applicable in third countries may not be equivalent to those arising under the NIA and may in certain instances be materially less stringent or differ in scope, application or interpretation. This may result in due diligence, screening or monitoring processes that are not sufficient to identify sanctions exposure in accordance with Maltese law.

The risk is therefore that the Operator may rely on information or checks that do not adequately capture the involvement of designated persons, including in particular where:

- The third-country regime does not apply the same ownership or control tests (including the aggregation of ownership interests);
- The scope of designated persons or restrictive measures differs from those applicable under EU or Maltese law;
- Screening is conducted against a narrower set of sanctions lists; or
- The approach to identifying beneficial ownership or control is less robust.

In such circumstances, reliance on intra-group entities in third countries may impair the Operator's ability to comply with its obligations under Article 5 and Article 32 of the NIA, including the obligation to ensure that funds or economic resources are not made available, directly or indirectly, to designated persons.

Operators should therefore ensure that any intra-group reliance arrangements involving entities established outside the EU are subject to enhanced scrutiny and that appropriate safeguards are in place. This may include, for example, requiring the application of EU and Maltese sanctions standards at group level, supplementing group-wide processes with additional controls, or performing independent verification of key elements of the due diligence.

Operators should not place reliance on intra-group entities in third countries where they are not satisfied that the information and checks performed are equivalent in substance and effectiveness to those required under the NIA.

9.1.2 Conditions for Outsourcing

Where an Operator outsources activities relating to Sanctions CDD or other sanctions-related controls, it should ensure that the outsourcing arrangement does not impair its ability to comply with its obligations under the NIA. In particular, the Operator should ensure that:

- The service provider is a reputable entity and has been subject to appropriate due diligence by the Operator prior to the outsourcing arrangement being established;

- The service provider performs the outsourced activities in accordance with the Operator's own policies, procedures and control standards;

- The Operator provides the service provider with clear and comprehensive procedures governing the performance of the outsourced activities and ensures that the provider is informed of any subsequent updates;

- The Operator is informed of any material changes to the service provider's systems, processes or arrangements that may affect the performance of the outsourced activities;

- The service provider notifies the Operator without delay of any sanctions matches, suspicions or adverse information identified in the course of performing the outsourced activities;

- All Sanctions CDD information and supporting documentation are properly maintained in accordance with applicable record-keeping requirements;

- All relevant records can be made available to the Operator without delay, including where required under Article 32(4) of the NIA;

- The service provider is required to notify the operators if they themselves become subject to non-compliance measures or criminal proceedings during the engagement;

- The service provider is required to undertake ongoing sanctions-related training to maintain an appropriate level of competence and awareness;

- Appropriate arrangements are in place to ensure that, in the event of termination of the outsourcing arrangement, all relevant records are transferred to the Operator; and

- The Operator is able to continue to discharge its legal and regulatory obligations without disruption following the termination of the outsourcing arrangement.

These arrangements should be clearly documented in a formal Outsourcing Agreement between the Operator and the Service Provider.

The SMB expects Outsourcing Agreements expressly to reflect the Operator's obligation to provide any information that may be requested by the SMB, irrespective of whether a process was performed by a third party. Operators should therefore ensure that such agreements include appropriate provisions requiring the service provider to make all relevant information and documentation available without delay.

Operators should retain signed Reliance and Outsourcing Agreements, together with any related correspondence, for the applicable record retention period (see Section 8 for further information).

9.2 Ongoing Oversight of Reliance and Outsourcing Arrangements

Operators should ensure that reliance and outsourcing arrangements are subject to appropriate ongoing oversight. Such arrangements should not be treated as a one-off exercise at the point of engagement but should be monitored on an ongoing basis to ensure that they continue to operate effectively and remain consistent with the Operator's obligations under the NIA.

Operators should therefore implement measures to monitor the performance of third parties and outsourced service providers and to ensure that the controls performed on their behalf continue to meet the required standards.

In particular, Operators should ensure that:

- Periodic reviews are conducted to assess whether the third party or service provider continues to meet the standards expected by the Operator;
- The effectiveness of the controls performed by the third party or service provider is subject to periodic testing or assurance;
- The Operator remains informed of any material changes to the third party's systems, procedures or compliance arrangements that may affect the performance of the relevant activities;
- Appropriate management information is obtained to enable the Operator to assess the quality and timeliness of the activities performed by the third party; and
- Any deficiencies or weaknesses identified are addressed promptly, including where necessary through remedial actions or the termination of the arrangement.
- Operators should also ensure that oversight arrangements are documented and that appropriate records are maintained demonstrating how reliance and outsourcing arrangements are monitored in practice.
- Operators should retain signed Reliance and Outsourcing Agreements, together with any related correspondence, for the applicable record retention period (see Section 8 for further information).

9.3 Prohibited Reliance and Outsourcing

Reliance or outsourcing arrangements are not permitted:

- Where the third party providing the relevant services is established in a jurisdiction that does not provide an adequate level of regulatory oversight or that presents heightened sanctions or financial crime risks, such as the FATF black and grey lists; or
- In the case of intra-group reliance or outsourcing where the standards applied by the entity providing the services do not meet standards required under the NIA and the guidance issued by the SMB.

BORD TA' SORVELJANZA DWAR IS-SANZJONIJIET
SANCTIONS MONITORING BOARD
MALTA

Chapter 10 Training and Awareness

10. Training and Awareness

Operators must ensure that relevant personnel possess adequate knowledge of applicable sanctions obligations and are able to apply the Operator's sanctions controls effectively in practice. To achieve this, Operators must provide regular and targeted training to staff involved in activities that may give rise to sanctions exposure. This includes personnel responsible for customer onboarding, sanctions screening, transaction processing, compliance oversight and reporting.

There is no prescribed frequency for staff training. Operators should be able to demonstrate that the frequency, scope, and content of their training programmes have been determined having regard to their operational environment and sanctions risk exposure. Training programmes should be designed to ensure that staff understand both the legal requirements of sanctions regimes and the Operator's internal procedures for complying with those requirements.
In particular, training programmes should:

- Be tailored to the employee's role, seniority and exposure to sanctions risk;
- Cover the key provisions of applicable sanctions legislation, including prohibitions, derogations, exemptions and potential penalties for non-compliance;
- Explain the Operator's internal procedures for sanctions screening, escalation and reporting;
- Include practical examples or case studies, where appropriate, to help staff recognise sanctions risks and respond to potential breaches; and
- Be refreshed periodically, particularly following changes in applicable legislation, sanctions regimes or internal procedures.

Operators should also ensure that training is provided to new staff members whose roles involve sanctions-related responsibilities. Records of sanctions training must be maintained. These records should demonstrate that relevant personnel have received appropriate instruction and that training is updated where necessary to reflect changes in sanctions obligations or the Operator's internal controls. Senior management should periodically review training arrangements to ensure that staff remain adequately informed of their responsibilities under sanctions legislation.

Chapter 11
Systems

11. Systems

To perform the Sanctions CDD controls described in Section 4, Operators will typically need to utilise one or more sanctions screening systems and, where relevant, transaction monitoring systems.

The use of automated systems is not mandatory. Operators are required to implement systems and processes that are proportionate to the nature, size and risk exposure of their activities. In determining the appropriate approach, Operators should have regard to their business model, client base and the nature and volume of their transactions.

Automated screening tools are typically more suitable for Operators with a large number of clients, high transaction volumes or greater exposure to international activity. Such systems can facilitate ongoing screening and enable more timely identification of potential matches or transactions that may give rise to sanctions concerns. Manual screening processes may be acceptable for smaller Operators with a limited number of clients and lower exposure to higher risk jurisdictions or complex transactions. However, where manual processes are adopted, Operators should ensure that screening is conducted consistently, documented appropriately and subject to adequate oversight.

Where an Operator adopts automated sanctions screening or transaction monitoring systems, it should ensure that these systems are implemented, calibrated and overseen in a robust manner, as described below.

11.1 Implementation of Screening and Monitoring Systems

Operators should exercise appropriate care when implementing sanctions screening or transaction monitoring systems to ensure that the systems are suitable for the Operator's business model and risk profile. Implementation should involve an assessment of whether the system is capable of supporting the Operator's sanctions compliance obligations, taking into account factors such as the nature of the Operator's clients, the jurisdictions in which it operates and the expected volume and complexity of transactions.

Operators should also ensure that responsibilities for the operation and oversight of the system are clearly defined and that staff responsible for the system are appropriately trained.

11.2 Calibration and Configuration

Operators should ensure that screening and monitoring systems are appropriately configured and calibrated so that they are capable of identifying potential sanctions risks while avoiding unnecessary or excessive alerts. Where automated systems are used, this includes the configuration of matching algorithms, such as fuzzy logic settings, as well as the calibration of thresholds, parameters and monitoring rules. Calibration should be undertaken carefully and should reflect the Operator's SRA. Systems that are configured too narrowly may fail to detect relevant risks, while systems that generate excessive alerts may undermine the effectiveness of the review process. Operators should therefore periodically review and adjust system parameters where necessary to ensure that systems remain effective.

11.3 Transparency and Explainability of System Rules and Algorithms

Operators should ensure that the rules, parameters and algorithms applied within sanctions screening and transaction monitoring systems are sufficiently transparent and capable of being explained.

In particular, Operators should ensure that they are able to understand and explain how the system identifies potential matches or generates alerts. This includes understanding the logic applied by matching algorithms, the configuration of fuzzy matching parameters and the monitoring rules used to identify potentially relevant transactions.

Where third party systems or vendor solutions are used, Operators should ensure that they obtain sufficient information from the provider to understand how the system operates and how alerts are generated. Operators should not rely on systems where the underlying logic cannot be reasonably understood or explained.

Operators should also maintain appropriate documentation describing the configuration of system rules, thresholds and algorithms. Such documentation should enable the Operator to demonstrate to the SMB that the system has been implemented and calibrated in a manner that is appropriate to its risk profile.

11.4 Ongoing Maintenance and Updating

Operators should ensure that sanctions screening and transaction monitoring systems are maintained and updated on an ongoing basis.

This includes ensuring that relevant sanctions lists and data sources are kept up-to-date, that system functionality is maintained and that any changes to the Operator's business model, customer base or risk exposure are appropriately reflected in system settings and monitoring rules.

Operators should also ensure that any material changes to systems or configurations are documented and, where appropriate, subject to internal approval.

11.5 Testing and Effectiveness Reviews

Operators should periodically test the performance of their sanctions screening and transaction monitoring systems to assess whether they operate effectively in practice. Testing may include the review of system parameters, analysis of alert volumes and outcomes, and sample testing to assess whether systems are capable of identifying relevant sanctions risks.

The purpose of such testing is to assess whether the systems remain appropriately calibrated and whether they continue to operate in a manner consistent with the Operator's sanctions risk profile. Where deficiencies are identified, Operators should take appropriate remedial action, including adjusting system settings, enhancing procedures or implementing additional controls where necessary.

Chapter 12
Governance

12. Governance

Effective sanctions compliance requires appropriate governance arrangements within the organisation. Operators must establish governance arrangements that provide effective oversight of sanctions compliance.

Governance arrangements mean, collectively:

- The clear allocation of responsibilities across the Three Lines of Defence model (a governance framework that allocates risk management responsibilities across operational management (i.e. the business, known as the First Line of Defence, oversight functions (typically Risk and Compliance functions known as the Second Line of Defence), and independent assurance (Internal Audit, the Third Line of Defence);

- The establishment and operation of oversight by senior management or designated committees;

- The establishment and operation of escalation and reporting mechanisms;

- The appointment and authority of the Sanctions Compliance Officer ("SCO");

- The review of Sanctions Framework's effectiveness; and

- The ongoing maintenance, updating and enhancement of the Sanctions Framework.

These arrangements should ensure that sanctions obligations are clearly understood and implemented across relevant business areas and that sanctions controls operate effectively in practice.

Senior management must ensure that adequate resources, systems and procedures are in place to support sanctions compliance. Sanctions risks should be considered as part of the Operator's overall risk management framework and should be subject to appropriate internal oversight.

12.1 Responsibilities Across the Three Lines of Defence

Operators should ensure that roles and responsibilities are allocated across the three lines of defence so that sanctions risks are appropriately identified, managed and independently overseen.

Responsibilities will typically be allocated along the following lines, although the precise allocation may vary depending on the Operator's size, structure and operating model. The First Line of Defence (i.e. the Business functions) gives rise to sanctions risk by way of the products and services it provides, and the clients to which it provides them. It is therefore expected to manage these sanctions risks by establishing policies and designing and applying adequate controls, documenting them in procedures.

The Second Line of Defence (typically, the Risk and Compliance functions) is responsible for acting as a point of escalation (e.g. to decide whether a potential match with a designated entity is confirmed) and provide guidance and conducting assurance over the controls established by the business.

The Third Line of Defence (Internal Audit) provides independent periodic assurance over the design adequacy and effectiveness of the Sanctions Framework as a whole (i.e. over the activities of the First and Second Line of Defence, together). There is no prescribed frequency for audit arrangements. Operators should be able to demonstrate that the frequency, scope, and coverage of internal audits (or external audits, where these functions are outsourced) are commensurate with their operational environment and risk exposure.

While certain activities supporting the Sanctions Framework, such as screening operations, quality assurance or independent testing, may be outsourced to third parties, Operators remain ultimately responsible for compliance with their sanctions obligations. The outsourcing of functions does not transfer accountability for the management of sanctions risk. Operators should therefore ensure that appropriate oversight arrangements are in place to monitor the performance of any outsourced activities and to ensure that sanctions risks continue to be identified, managed and controlled effectively (see Section 9 for additional information).

12.2 The Role of Senior Management

Senior management plays a central role in ensuring that the Operator complies with its sanctions obligations and that sanctions risks are appropriately identified, managed and overseen. Senior management should ensure that the Operator maintains an effective Sanctions Framework that is proportionate to the nature, scale and complexity of its activities.

In particular, senior management should:

- Approve the Operator's sanctions policies and procedures and ensure that they are reviewed periodically and updated where necessary;

- Ensure that an SRA is conducted and that appropriate controls are implemented to address the risks identified;

- Allocate clear responsibility for sanctions compliance within the organisation and ensure that individuals responsible for sanctions compliance have sufficient authority, resources and independence to perform their functions effectively;

- Ensure that appropriate systems and controls are in place to identify and manage sanctions risks, including screening, escalation and reporting procedures;

- Receive and review management information relating to sanctions compliance, including information on potential matches, breaches, control weaknesses and remedial actions;

- Ensure that staff receive appropriate training to enable them to understand and comply with the Operator's sanctions obligations; and

- Promote a culture of compliance in which sanctions obligations are understood and treated as a core component of the Operator's legal and regulatory responsibilities.

Operators should consider incorporating sanctions compliance objectives into the performance evaluation of relevant senior management, so as to reinforce accountability for the effective management of sanctions risks.

12.3 Oversight by Senior Management or Designated Committees

Operators should establish arrangements to ensure that sanctions compliance is subject to appropriate oversight at senior management level. This oversight may be exercised directly by senior management or through a designated committee responsible for compliance, risk or financial crime matters.

Oversight arrangements should ensure that senior management receives sufficient information to enable it to assess the effectiveness of the Sanctions Framework and to take informed decisions where issues arise. In particular, Operators should ensure that:

- Sanctions compliance is included as a standing item within relevant governance forums where appropriate;
- Senior management or the designated committee receives regular reporting on sanctions risk, controls and compliance matters;
- Significant issues, including potential sanctions breaches or control weaknesses, are brought promptly to the attention of senior management; and
- Decisions and actions relating to sanctions compliance are appropriately documented

12.4 Escalation and Reporting Mechanisms

Operators should establish clear internal escalation and reporting mechanisms to ensure that sanctions-related issues are identified, assessed and addressed in a timely manner. These arrangements should ensure that staff understand to whom, when, and how to escalate potential sanctions concerns, and that such matters are assessed by individuals with the appropriate authority and expertise.

In particular, Operators should ensure that:

- Procedures are in place for the escalation of potential sanctions matches or other sanctions-related concerns identified in the course of business activities;
- Responsibilities for reviewing and assessing escalated matters are clearly defined;

- Clear decision-making processes are established for determining whether measures such as the freezing of funds or reporting to competent authorities are required; and

- Records are maintained of escalations, decisions taken and actions implemented.

12.5 Appointment of a Sanctions Compliance Officer

To ensure accountability and effective implementation of sanctions controls, Operators should designate a Sanctions Compliance Officer (SCO) or assign equivalent responsibility within the compliance function.

The SCO (or equivalent) should have sufficient authority, independence and resources to oversee the Operator's Sanctions Framework and should report directly to senior management or the board of the Operator.

The SCO should be responsible for overseeing the implementation and operation of sanctions controls, including:

- Ensuring that sanctions policies and procedures are implemented and applied consistently across the organisation;

- Overseeing sanctions screening and monitoring processes;

- Reviewing and escalating potential sanctions matches; and

- Acting as the primary point of contact with the SMB, where required.

Notwithstanding the designation of an SCO, senior management retains overall responsibility for ensuring compliance with sanctions obligations.

12.6 Reviewing the Effectiveness of the Sanctions Framework

Operators should periodically review the effectiveness of their Sanctions Framework to ensure that it remains appropriate to the nature, scale and complexity of their activities and to the sanctions risks to which they are exposed and that it demonstrably manages the risk to which they are exposed.

Such reviews should consider whether the policies, procedures and controls established by the Operator are appropriately designed and whether they operate effectively in practice. The purpose of this exercise is not only to confirm compliance with applicable sanctions obligations but also to identify weaknesses, gaps or areas where controls may require strengthening.

12.7 Integration of the Sanctions Framework

For a Sanctions Framework to operate effectively, its various components should not be treated as separate or isolated processes. Instead, they should operate as part of a coherent and continuous system in which each element informs and supports the others.

In practice, this means that the different components of the framework such as the SRA, Sanctions CDD, sanctions screening, transaction monitoring, escalation procedures and reporting arrangements should be designed to operate as a continuum. The outputs of one component should inform the operation of the others, creating a feedback mechanism through which Operators are able to refine their understanding of sanctions risk and adjust their controls where necessary.

For example, information obtained through screening activities, transaction monitoring alerts, internal investigations or the review of sanctions hits may reveal patterns, vulnerabilities or emerging risks. These insights should be reflected in the Operator's SRA and, where appropriate, lead to adjustments to policies, procedures or monitoring rules.

Conversely, the results of the SRA should inform how controls are designed, prioritised and applied in practice. Higher-risk activities, jurisdictions or client profiles identified through the risk assessment may require enhanced controls, more frequent screening or more intensive transaction monitoring. Operators should also ensure that the Sanctions Framework is actively used as a decision-making tool rather than a purely formal control environment. Information generated through the various components of the framework should inform operational decisions, including:

- Whether to establish or maintain a business relationship;
- Whether a transaction should proceed or requires further review;

- Whether enhanced controls or monitoring measures are required; and
- Whether escalation or reporting to competent authorities is necessary.

Governance arrangements should ensure that relevant functions within the organisation are able to share information generated through the Sanctions Framework and that lessons derived from operational experience are incorporated into the ongoing management of sanctions risk.

12.8 Ongoing Maintenance, Updating and Enhancement of the Sanctions Framework

Sanctions Frameworks should be dynamic and capable of adapting to changes in sanctions regimes, regulatory expectations and the Operator's own activities. Operators should therefore establish processes to ensure that relevant developments are identified and incorporated into their Sanctions Framework in a timely manner. In particular,

Operators should:

- Monitor changes in applicable legislation, sanctions lists and guidance issued by competent authorities;
- Update internal policies, procedures and systems where necessary to reflect those developments; and
- Ensure that relevant staff are informed of changes that may affect the implementation of sanctions controls.

Operators should also maintain appropriate channels of communication with the SMB and, where relevant, with other competent authorities or industry bodies. Such engagement can assist Operators in remaining informed about regulatory expectations and emerging risks.

Annexes

BORD TA' SORVELJANZA DWAR IS-SANZJONIJIET
SANCTIONS MONITORING BOARD
MALTA

Annex 1

Administrative Penalties and Criminal Offences for Breaches of Sanctions (Restrictive Measures) Obligations

This Annex provides a consolidated overview of the enforcement provisions contained in NIA that are relevant to breaches of restrictive measures.

The purpose of this Annex is to summarise, in a structured and accessible form, the principal legal consequences that may arise where restrictive measures are breached or where obligations under the NIA are not complied with. These include criminal offences, administrative penalties, and the procedures through which such penalties may be imposed, settled, appealed or enforced.

The Annex is intended as a reference tool to assist Operators and other readers of this Guidance Note in understanding the legal framework governing sanctions enforcement in Malta. The provisions summarised in this Annex are drawn directly from the NIA and include, in particular, Articles 7, 9 to 14, 29, 35, 37 and 38.

Throughout this section Articles mean Articles of the NIA.

Article 7: Performance of Obligations

Article 7 sets out the legal consequences that restrictive measures have on transactions and contractual obligations.

First, persons, entities and bodies in Malta are prohibited from entering into transactions or assuming new obligations where the performance of those transactions or obligations would contradict restrictive measures imposed under EU law, UN Security Council Resolutions or domestic restrictive measures implemented under the NIA.

Second, where restrictive measures are in force, it is prohibited to perform transactions or obligations whose performance would contradict those restrictive measures.

Third, where transactions or obligations were entered into prior to the adoption of restrictive measures but their performance subsequently becomes incompatible with those measures, the relevant transactions or obligations must be terminated without delay, or their performance must be suspended for the duration of the restrictive measures.

The Article also clarifies that persons, entities or bodies will not incur civil liability for the non-performance of transactions or obligations where such non-performance results from compliance with restrictive measures.

Finally, the Article provides that losses incurred as a result of lawful actions taken by the SMB in the implementation of the NIA are not compensable.

Obligation Type	What Is Prohibited?	Legal Effect	Liability/ Compensation
New Transactions / Obligations	If they contradict restrictive measures	Prohibited (or perform such obligations may expose the parties to sanctions, including administrative or criminal liability.)	No civil liability
Existing Transactions	Must be terminated or suspended if now prohibited	Terminated or Suspended	No compensation for losses

Article 9: Criminal Offences

Article 9 establishes the criminal offences associated with breaches of restrictive measures.

In particular, it provides that a person commits a criminal offence where they intentionally engage in conduct that violates restrictive measures imposed under EU law, UN Security Council Resolutions or domestic measures adopted under the NIA. This includes, among other things, making funds or economic resources available to designated persons, failing to comply with freezing obligations, enabling designated persons to enter or transit through Malta where prohibited, carrying out prohibited transactions or trade activities, or circumventing restrictive measures through concealment, misrepresentation or other deceptive conduct.

The Article also introduces a distinction between criminal offences and administrative infringements based on the value involved in the breach. Where the value of the funds, assets or economic resources involved in the conduct is below €10,000, the breach may be treated as an administrative failure rather than pursued as a criminal offence.

Conduct	Classification where value > EUR10,000	Possible classification where value <EUR10,000
Making funds or economic resources available to designated persons or entities	Criminal offence	May be treated as an administrative infringement
Failure to freeze funds or economic resources belonging to a designated person	Criminal Offence	May be treated as an administrative infringement
Carrying out transactions prohibited under restrictive measures	Criminal offence	May be treated as an administrative infringement
Trading, importing, exporting, brokering or providing services in breach of restrictive measures	Criminal Offence	May be treated as an administrative infringement
Circumventing restrictive measures (e.g. concealment of assets or provision of false information)	Criminal Offence	May be treated as an administrative infringement

Conduct	Classification where value > EUR10,000	Possible classification where value <EUR10,000
Allowing entry or transit of designated persons where prohibited	Criminal Offence	May be treated as an administrative infringement
Trading, importing, exporting, brokering or providing services in breach of restrictive measures	Criminal offence	May be treated as an administrative infringement
Circumventing restrictive measures (e.g. concealment of assets or provision of false information)	Criminal offence	May be treated as an administrative infringement
Allowing entry or transit of designated persons where prohibited	Criminal offence	Not value-based
Humanitarian assistance carried out in accordance with international principles	Not an offence	Not an offence
Information obtained by legal professionals in the course of legal advice or representation	Not an offence	Not an offence

Article 10: Inciting, Aiding, and Abetting

Article 10 establishes liability for persons who participate in the commission of offences under Article 9, as well as for attempts to commit such offences.

A person who incites, aids or abets the commission of an offence under Article 9 is subject to the same penalties as the principal offender.

The Article also addresses attempted offences. Where a person begins to commit an offence, but the offence is not completed due to causes independent of the person's will, the applicable penalty may be reduced. Where the person voluntarily abandons the attempt before the offence is completed, liability is limited to the acts that were actually carried out.

Action Type	Liability	Penalty Consequences	Notes
Inciting the commission of an Article 9 offence	Criminal liability	Same Penalty as the principal offender	Applies even if the person does not commit the offence directly
Aiding or abetting an Article 9 offence	Criminal liability	Same penalty as the principal offender	Covers assistance or facilitation
ttempt to commit an Article 9 offence (offence not completed due to external causes)	Criminal liability	Penalty may be reduced	Reduction typically by one or two degrees
Attempt to commit an Article 9 offence (voluntarily abandoned)	Limited liability	Penalty applies only to acts actually committed	No liability for the intended offence if abandoned voluntarily

Article 11: Punishments for Criminal Offences

Article 11 establishes the penalties applicable to criminal offences committed under the NIA.

Natural persons who commit offences under Article 9 may be subject to substantial financial penalties, imprisonment, or both. Where the value of the funds, assets or economic resources involved exceeds €100,000, higher minimum penalties may apply.

Legal persons may also be held liable for offences committed for their benefit. In such cases, financial penalties may be imposed either as a percentage of the legal person's total worldwide turnover or, where turnover cannot be determined, within fixed monetary ranges established by the NIA.

In addition to financial penalties, courts may impose a range of additional measures. These may include the suspension or withdrawal of licenses, closure of establishments, exclusion from public benefits or funding, judicial supervision or compulsory winding up.

Directors, managers and other officers of a legal person may incur personal liability where the offence was committed with their knowledge or where they failed to exercise appropriate supervision or due diligence.

The Article also provides for adjustments to penalties where aggravating or mitigating circumstances exist. Penalties may be increased in situations involving organised criminal activity, use of forged documents or repeat offences, and may be reduced where the offender cooperates with the competent authorities.

Offender	Penalty Framework	Additional measures	Notes
Natural Persons	Fine from €25,000 to €5,000,000, imprisonment up to 12 years, or both	Possible additional sanctions imposed by the court	Higher minimum penalties may apply where value ≥ €100,000
Legal Persons	Fine of 1%–5% of total worldwide turnover, or €80,000–€10,000,000 where turnover cannot be determined	Suspension or withdrawal of licences, closure of establishments, exclusion from public benefits, judicial supervision, compulsory winding up	Applies where offence committed for benefit of legal person
Directors, managers and officers	Personal liability may arise	Same penalties as applicable to the offence	Liability may be avoided if due diligence and lack of knowledge are demonstrated
Aggravating circumstances	Penalties may be increased	/	Includes organised criminal activity, forged documents, repeat offences
Mitigating circumstances	Penalties may be reduced	/	Includes cooperation with authorities

Articles 12 and 13: Special Mechanisms for Out of Court Settlements

Article 12: Out of Court Settlement Before Criminal Proceedings Begin

Article 12 establishes a mechanism that allows certain breaches of the NIA to be resolved through an out of court settlement before criminal proceedings are instituted.

Under this provision, a person, entity or body that has committed a breach of the NIA may submit a written request to the SMB seeking to resolve the matter through an administrative settlement. If the SMB considers that the conditions for settlement are satisfied, it may enter into a settlement agreement with the person concerned.

The settlement agreement sets out the administrative penalty and any additional measures that must be fulfilled. Once the agreement is signed and the terms of the agreement are fully complied with, criminal proceedings may no longer be instituted in respect of the breach.

The Article also establishes procedural rules governing the settlement process, including time limits for the issuance of a draft settlement agreement and for its acceptance by the person concerned. Where the conditions of the settlement agreement are not fulfilled, the SMB must refer the matter to the Executive Police, and criminal proceedings may then be pursued.

Situation	Mechanism	Consequence	Notes
Breach of the NIA identified before criminal proceedings begin	Person may submit written request to SMB for settlement	SMB may propose Settlement agreement	Applies before criminal proceedings are instituted
Settlement agreement concluded	Administrative penalty and any additional measures imposed	Criminal proceedings cannot be instituted once conditions are fulfilled	Settlement must be fully complied with

Settlement agreement not fulfilled	SMB refers matter to Executive Police	Criminal proceedings may follow	Settlement protections no longer apply
Settlement penalty level	Administrative penalty determined in agreement	Capped at a proportion of the maximum applicable penalty	Determined by SMB

Situation	**Conditions/Requirements**	**Penalty/Effect**
Eligibility for settlement	First-time offender or no use of Art. 12/13 mechanism in previous 5 years	May request administrative settlement
SMB issues draft agreement	Within 1 month of request (extendable once by 1 month)	Details breach, penalty, obligations
Signature deadline	1 month from notification (extendable once)	Must sign to proceed with settlement
Penalty level	Up to ½ of maximum administrative penalty	Criminal liability extinguished upon full compliance
Failure to comply	SMB reports to Executive Police	Criminal proceedings may commence
Full compliance	Administrative penalty and measures completed	No further charges for the same breach

Article 13: Out of Court Settlement After Criminal Proceedings Have Been Instituted

Article 13 establishes a mechanism that allows certain breaches of the NIA to be resolved through an out of court settlement even after criminal proceedings have been instituted.

Under this provision, where criminal proceedings have already commenced in respect of a breach of the NIA, the person, entity or body concerned may request that the matter be resolved through a settlement with the SMB. If the conditions established under the Article are satisfied, the SMB may enter into a settlement agreement with the person concerned.

The settlement agreement sets out the administrative penalty and any additional measures that must be fulfilled. Where the settlement agreement is concluded and its terms are fully satisfied, the criminal proceedings in respect of the breach are discontinued.

The Article also establishes procedural rules governing the settlement process, including time limits for the submission and acceptance of settlement agreements. If the conditions of the agreement are not fulfilled, the settlement mechanism ceases to apply and the criminal proceedings may continue.

Situation	Mechanism	Consequence	Notes
Criminal proceedings already instituted for a breach of the NIA	Person may request settlement with SMB	SMB may propose settlement agreement	Applies after criminal proceedings have begun
Settlement agreement concluded	Administrative penalty and any additional measures imposed	Criminal proceedings cannot be instituted once conditions are fulfilled	Settlement must be fully complied with

Settlement agreement not fulfilled	Settlement protection no longer applies	Criminal proceedings may continue	Matter remains before the courts
Settlement penalty level	Administrative penalty determined in agreement	Subject to limits established under the NIA	Determined by SMB

Stage	Conditions/Requirements	Penalty/Effect
Eligibility	Must be currently charged in court; no prior use in last 5 years	May request settlement
SMB Response	Within 1 month (extendable once)	Issues notice + draft agreement
Contents of Agreement	Admissions, penalty, obligations, deadlines	Becomes executable title
Penalty level	Up to 7/10 of maximum applicable criminal punishment	Paid in lieu of continued prosecution
Court involvement	Court suspends proceedings during fulfilment	Court extinguishes criminal action once obligations completed
Non-fulfilment	Agreement used as proof of admission	Criminal case resumes
Multiple accused	Applies only to those who enter settlement	Proceedings split if necessary

Overall Comparison of Articles 12 and 13

Feature	Article 12	Article 13
Stage of Proceedings	Before criminal proceedings are instituted	After criminal proceedings have been instituted
Who initiates settlement	Person, entity or body requests settlement	Person, entity or body requests settlement
Authority entering settlement	Sanctions Monitoring Board	Sanctions Monitoring Board
Effect of successful settlement	Criminal proceedings cannot be instituted	Existing criminal proceedings are discontinued
Court role	No court involvement (proceedings not yet instituted)	Must approve and suspend proceedings
Maximum penalty	½ of maximum administrative penalty	Administrative penalty capped at 7/10 of the maximum criminal penalty
Effect of compliance	Criminal proceedings cannot be instituted	Court extinguishes criminal action
Failure to comply with settlement	Matter referred to Executive Police	Criminal proceedings continue

Article 14: Administrative Penalties for Minor Offences

Article 14 establishes the administrative penalty regime applicable to minor breaches of restrictive measures.

Under this provision, the SMB may impose administrative penalties where a breach of restrictive measures does not warrant criminal prosecution or where the law provides that the breach may be treated as an administrative infringement.

Administrative penalties under this Article may be imposed on persons, entities or bodies in Malta that fail to comply with restrictive measures or related obligations established under the NIA.

The purpose of this mechanism is to enable breaches of a less serious nature to be addressed through administrative enforcement rather than criminal proceedings.

The imposition of administrative penalties does not prevent the SMB from taking additional supervisory or enforcement measures where appropriate.

Offender Type	Maximum Penalty (as % of value involved)	Personal Liability?
Natural person	15%	Yes, unless the person demonstrates that they lacked knowledge of the breach and exercised all reasonable diligence to prevent it.
Legal person	35%	Directors or managers may incur personal liability where the breach occurred with their knowledge or due to lack of supervision.

Article 30(6): Failure to Comply with the SMB's Requests

Article 30(6) establishes an administrative penalty for failure to comply with requests issued by the SMB in the exercise of its powers under the NIA.

Under this provision, persons, entities or bodies that fail to provide information, documents or assistance requested by the SMB, or that otherwise fail to comply with a lawful request made in the course of the SMB's supervisory or investigative functions, may be subject to an administrative penalty. This obligation supports the ability of the SMB to monitor compliance with restrictive measures and to carry out investigations where potential breaches are identified.

Administrative penalties imposed under this provision are intended to ensure that persons, entities and bodies cooperate fully with the SMB and comply with requests issued in the exercise of its statutory powers.

Type of Failure	Penalty per Breach	Accumulation Rule
Failure to provide information or documents requested by the SMB	Up to €100	Initial administrative penalty may be imposed where a request is not complied with
Continued failure to comply following an SMB reminder or further request	Up to €100	Additional penalties may be imposed for each subsequent instance of non-compliance
Continued failure to comply following an SMB reminder or further request	Up to €100 per instance	Penalties may accumulate where repeated failures to comply occur

Article 35: Administrative Penalties in Relation to Article 32 Obligations

Article 35 establishes administrative penalties that may be imposed on Operators that fail to comply with obligations under Article 32 of the NIA.

Where an Operator breaches its obligations under Article 32, the SMB may impose an administrative penalty. These obligations include, among other things, the duty to comply with restrictive measures, to freeze funds or economic resources where required, and to report relevant information to the competent authorities.

The Article also provides that liability may extend to directors, managers or other officers of a legal person where the breach occurred with their knowledge or where it resulted from a failure to exercise appropriate supervision or due diligence. Administrative penalties imposed under this Article are intended to ensure compliance by Schedule I operators with their sanctions obligations and may be applied in addition to other supervisory or enforcement measures available under the NIA.

Type of Breach	Penalty Range (€)	Who is Liable?
Standard Breach of Article 32	€100 – €500	Operators listed under Schedule I
Serious, repeated, or systematic breach	€300 – €1,500	Operators listed under Schedule I
Non-compliance with SMB directive	€100 – €500 (or as above)	Operators listed under Schedule I

Daily cumulative penalty	At least €100/day, max €2,500	Operators listed under Schedule I

When an administrative penalty is imposed, the SMB must promptly inform any relevant supervisory authority or other body responsible for authorizing, licensing, registering, or regulating the person or entity concerned, and provide all necessary information about the penalty. The SMB may also recommend that the relevant authority take further regulatory action as appropriate.

If the administrative penalty exceeds €1,500, it must be published on the SMB's website according to its policies and procedures.

Action by SMB	Who is Notified?	Publication Requirement
Imposes administrative penalty	Relevant supervisory authority/body	If penalty > €1,500, published on SMB website
Recommends further regulatory action	Supervisory authority/body	Based on facts / context of the case

Article 37: Appeals from Administrative Penalties

Article 37 establishes the right of appeal for persons, entities or bodies that consider themselves aggrieved by an administrative penalty imposed under the NIA.

This right of appeal applies to administrative penalties imposed under provisions such as Articles 14, 35 and 36 of the NIA, which provide for administrative enforcement in different contexts. The categories of penalties to which the appeal mechanism applies are summarised in the table below. Under Article 37, a person subject to an administrative penalty may appeal the decision before the Court of Appeal (Inferior Jurisdiction). Appeals may be brought on both points of law and points of fact.

The appeal must be filed within twenty working days from the date on which the administrative penalty is served on the person concerned. Proceedings before the Court of Appeal are conducted in camera in order to protect the confidentiality of sensitive information relating to sanctions enforcement. Alternatively, an appeal may be filed before the Tribunal in accordance with Article 19(8), providing the person, entity, or body with the option of avoiding recourse to the Court.

Administrative penalties under Article:	Who is Liable?	Key Steps and Deadlines	Notes
14	All persons, entities and bodies in Malta	Appeal to Court of Appeal (Inferior Jurisdiction) within 20 working days; heard in camera	Covers point of law and fact
35	Operators	Appeal to Court of Appeal (Inferior Jurisdiction) within 20 working days; heard in camera	Covers point of law and fact
36	Payment Services Providers	Appeal to Court of Appeal (Inferior Jurisdiction) within 20 working days; heard in camera	Covers point of law and fact

Article 38: Recovery of Administrative Penalties

Article 38 establishes the mechanism for the enforcement and recovery of administrative penalties imposed under the NIA.

Where an administrative penalty is not appealed within the prescribed period and remains unpaid twenty working days after service of the notice, the penalty becomes recoverable as a civil debt.

For this purpose, the written notice imposing the administrative penalty, once served by judicial act, constitutes an executive title. This means that the penalty may be enforced directly in accordance with the procedures applicable to the recovery of civil debts under the Code of Organisation and Civil Procedure.

Where an administrative penalty is appealed and subsequently confirmed, whether in whole or in part, the confirmed amount becomes enforceable in the same manner.

This provision ensures that administrative penalties imposed under the NIA may be enforced through the civil debt recovery framework where payment is not made voluntarily.

SMB BORD TA' SORVELJANZA DWAR IS-SANZJONIJIET
SANCTIONS MONITORING BOARD
MALTA

Annex 2

Examples in Practice: Identifying and Screening Parties in Complex Ownership and Control Structures

This Annex sets out a series of worked examples illustrating how the principles set out in Section 4 (Customer Due Diligence) apply to the identification and screening of parties in more complex ownership and control structures.

The examples are intended as a practical reference tool for Operators and other readers of this Guidance Note. They cover a range of structures encountered in practice, including private equity and investment fund structures, trusts, foundations, minority shareholdings combined with enhanced governance rights, listed companies, nominee arrangements, affiliate relationships, debt-based control, and crypto-asset service provider relationships.

For each example, the relevant ownership or control structure is set out together with an illustrative diagram, followed by an assessment of which parties it would be prudent for the Operator to screen and the reasoning underlying that assessment.

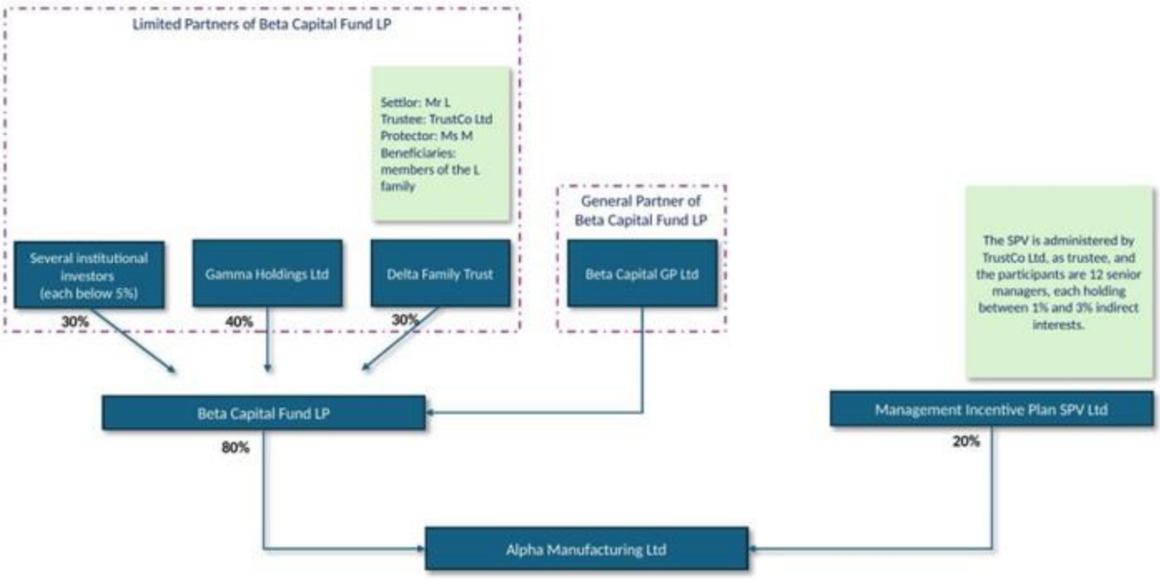
Example 1: Private equity fund with layered ownership and a trust

The client is Alpha Manufacturing Ltd. Alpha Manufacturing Ltd is 80% owned by Beta Capital Fund LP, a private equity fund. Beta Capital Fund LP has the following structure:

- General Partner: Beta Capital GP Ltd (controls the fund).
- Limited partners: Gamma Holdings Ltd (40%), Delta Family Trust (30%), Several institutional investors (each below 5%). The Operator ascertains that these investors do not exercise control by other means.

The Delta Family Trust has the following parties: Settlor: Mr L, Trustee: TrustCo Ltd, Protector: Ms M, Beneficiaries: members of the L family.

The other 20% of Alpha Manufacturing Ltd is held in Management Incentive Plan SPV Ltd. Management Incentive SPV Ltd represents equity allocated to the senior leadership team. The SPV is administered by TrustCo Ltd as trustee, and the participants are 12 senior managers, each holding between 1% and 3% indirect interests.



In light of the information known, it would be best practice for the Operator to screen:

- The client (Alpha Manufacturing Ltd) - The client should always be screened because it is the direct counterparty to the Operator.

- Beta Capital Fund LP - Because it holds a controlling ownership interest in the client (80%). Under sanctions rules, restrictions may apply not only to designated persons themselves but also to entities owned or controlled by designated persons. Screening the fund therefore allows the Operator to determine whether the client could indirectly be owned or controlled by a designated person through the fund structure.

- Beta Capital GP Ltd - Because it exercises control over the fund, even if it does not hold a significant economic interest in it. In private equity structures, the General Partner typically has authority over investment decisions and governance of portfolio companies. As a result, a designated person controlling the General Partner could indirectly exercise control over the client. Screening the General Partner therefore addresses the risk of control arising through governance rights rather than ownership.

In relation to Gamma Holdings Ltd and the Delta Family Trust, if both were designated persons they would together hold 70% of Beta Capital Fund LP. In that situation the fund would be considered owned by designated persons because designated persons collectively hold more than 50% of the ownership interests. Since Beta Capital Fund LP owns 80% of Alpha Manufacturing Ltd, Alpha Manufacturing Ltd would therefore be considered indirectly owned by designated persons.

If only one of them were designated, Beta Capital Fund LP would not be considered owned by designated persons, and Alpha Manufacturing Ltd would therefore not be considered owned by designated persons through the ownership test via Beta Capital Fund LP. However, Alpha Manufacturing Ltd could still be considered owned or controlled by a designated person if the designated person were found to exercise control over the fund or the client through other means, for example through governance rights, veto powers or other arrangements conferring dominant influence.

Because the two entities could, in aggregate, hold more than 50% of the ownership interests in Beta Capital Fund LP, the prudent course of action would be to screen both Gamma Holdings Ltd and the Delta Family Trust. If only one of them were found to be a designated person, the Operator should then determine whether that party exercises control through other means, such as governance rights, veto powers or other arrangements conferring dominant influence.

Because Delta Family Trust is a trust, the Operator should identify and screen the relevant parties associated with the trust, including the trustee and, where relevant, the settlor, protector and beneficiaries.

In relation to the Management Incentive Plan SPV Ltd, since the SPV holds only 20% of Alpha Manufacturing Ltd, even if the SPV itself were a designated person the client would not automatically be considered owned by a designated person under the 50% ownership rule. However:

- Even though the ownership rule cannot be triggered, the SPV could still create sanctions exposure because funds or economic resources could be made available to it. If the SPV itself were a designated person, dividends or other distributions from the client to the SPV could amount to making funds available to a designated person; and

- The SPV itself could be controlled by a designated person, even if it is not designated.

It would therefore be prudent for the Operator to screen the entity, as it is a direct shareholder of the client. If the SPV were found to be a designated person, the Operator would need to assess whether the relationship or any transactions carried out through the Operator could result in funds or economic resources being made available to the SPV and determine what restrictions or reporting obligations may therefore apply. However, the fact that it holds 20% rather than 50% means that the client would not automatically be considered owned by a designated person through the ownership rule.

The Operator should also identify and screen the party exercising control over the SPV. This is because sanctions measures apply not only to entities that are designated themselves, but also to entities that are owned or controlled by designated persons. Screening the person exercising control over the SPV therefore allows the Operator to determine whether the SPV itself may be controlled by a designated person.

In the context of a management incentive plan SPV, the party exercising control will typically be the trustee, the directors or managing entity of the SPV or another fiduciary or administrator responsible for managing the SPV and exercising the governance rights associated with the shares. Because these parties may exercise the rights attached to the shares held by the SPV, including voting rights and decisions relating to distributions, they may effectively control the SPV's participation in the client. Screening them therefore helps ensure that the SPV is not controlled, directly or indirectly, by a designated person.

In relation to the 12 senior managers participating in the management incentive plan (i.e. the individuals who ultimately benefit economically from the SPV), it will not normally be necessary to screen each of these individuals where they hold small indirect interests through the SPV and do not exercise control over the SPV or over the shares held by it. If, however, one or more of the senior managers were found to hold a significant economic interest in the SPV or to exercise influence over the SPV through governance rights, voting arrangements or other contractual mechanisms, the Operator should consider whether screening that individual would also be appropriate. Before deciding not to screen them, therefore, the Operator should satisfy itself that the senior managers do not exercise ownership or control over the SPV or over the shares held by it. This may involve reviewing the relevant governance arrangements for the SPV, including any shareholder agreements, trust deeds, participation agreements or other documentation governing the management incentive plan, in order to determine whether any participant holds voting rights, veto powers or other rights capable of conferring influence over the SPV or its shareholding in the client. The Operator should also document the basis on which it concluded that screening those individuals was not necessary.

In relation to the institutional investors participating in Beta Capital Fund LP, each holding an interest of less than 5%, it will not normally be necessary for the Operator to screen each of these investors where they hold small, passive interests and do not exercise control over the fund or over the client.

In most private equity structures, institutional investors participate as limited partners whose rights are limited to providing capital and sharing in the economic returns of the fund. They typically do not participate in the management of the fund, do not exercise voting rights in relation to portfolio companies and do not have the ability to direct the fund's investment decisions.

In such circumstances, the Operator may reasonably conclude that these investors do not create sanctions exposure for the purposes of the relationship with the client. The relevant parties to screen will generally be the fund itself and the entity exercising control over it, such as the General Partner or investment manager.

However, the Operator should remain alert to situations where an investor holding a minority interest may nevertheless exercise influence over the fund. For example, an investor may hold governance rights, veto rights or other contractual rights capable of influencing the fund's investment decisions or its management of portfolio companies.

Before deciding not to screen these investors, therefore, the Operator should satisfy itself that they hold purely passive interests and do not exercise ownership or control over the fund. This may involve reviewing the relevant governance documentation of the fund, including the limited partnership agreement or any side letters, to determine whether any investor holds rights capable of conferring influence over the fund or its investments. The Operator should also document the basis on which it concluded that screening those investors was not necessary.

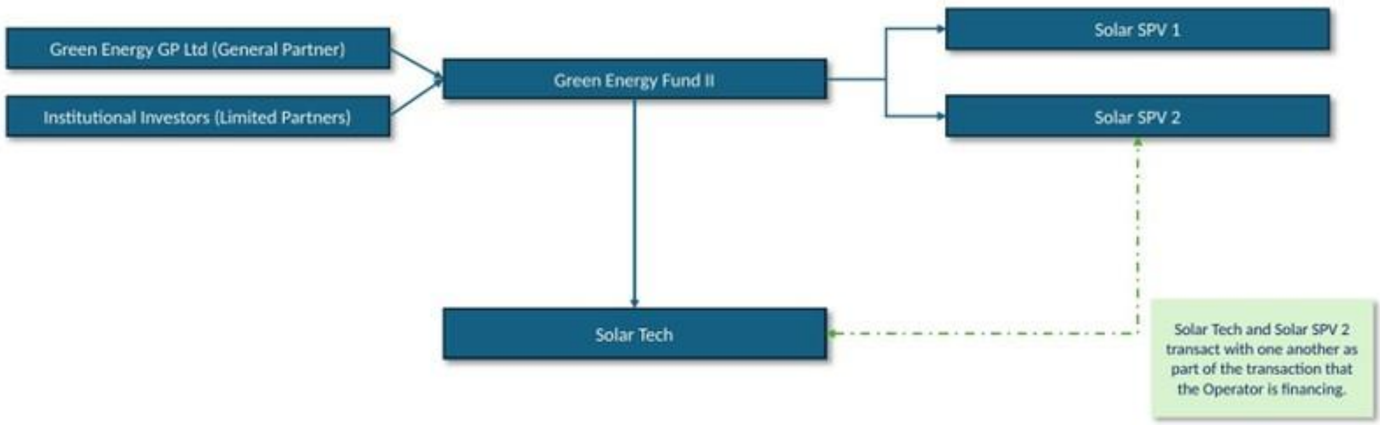
Example 2: Investment fund transacting with subsidiaries

The client is SolarTech Ltd. SolarTech Ltd is wholly owned by Green Energy Fund II. Green Energy Fund II has the following structure:

- General Partner: Green Energy GP Ltd, which is responsible for managing the fund and exercising control over its affairs.

- Limited partners: several institutional investors, each holding limited partner interests. The Operator ascertains, on the basis of the fund documentation and the information available, that these investors are passive investors and do not exercise control over the fund or over SolarTech Ltd through governance rights or other means.

Green Energy Fund II also owns a number of special purpose subsidiaries established for different projects, including Solar SPV 1 Ltd and Solar SPV 2 Ltd. Neither Solar SPV 1 Ltd nor Solar SPV 2 Ltd holds an ownership interest in SolarTech Ltd. However, SolarTech Ltd transacts with Solar SPV 2 Ltd as part of a project that the Operator is financing (funds, services or economic resources may therefore flow between the client and Solar SPV 2 Ltd in the course of the relationship).



In light of the information known, it would be prudent for the Operator to screen:

- SolarTech Ltd - The client should always be screened because it is the direct counterparty to the Operator. This is the starting point of the sanctions assessment and is necessary to determine whether the client itself is a designated person or otherwise subject to restrictive measures.

- Green Energy Fund II - The fund should be screened because it is the direct owner of the client. Where a legal entity is owned by another entity, sanctions exposure may arise not only where the owner itself is designated, but also where the owner is owned or controlled by a designated person. Screening the fund therefore enables the Operator to assess whether the client may be owned or controlled, directly or indirectly, by a designated person through the fund structure. If Green Energy Fund II itself were a designated person, or if it were found to be owned or controlled by a designated person, SolarTech Ltd could itself be treated as subject to sanctions restrictions depending on the application of the ownership and control tests. Screening the fund is therefore necessary to understand whether the client may be indirectly caught.

- Green Energy GP Ltd - The General Partner should also be screened because it exercises control over the fund, even if it does not hold the principal economic interest in it. In fund structures, control often arises through governance and management rights rather than through ownership alone. The General Partner will typically have authority over the fund's investments, its subsidiaries and, in practical terms, the exercise of shareholder rights in relation to portfolio companies. Accordingly, even if Green Energy Fund II were not itself designated, a designated person exercising control over Green Energy GP Ltd could create sanctions exposure through the fund's governance structure.

- Solar SPV 2 Ltd - Although not in the ownership chain of the client, Solar SPV 2 Ltd should be screened because it is a party directly involved in the transaction. This is important because sanctions exposure does not arise only through ownership and control. It may also arise where funds or economic resources are made available, directly or indirectly, to a designated person.

If Solar SPV 2 Ltd were itself a designated person, or were owned or controlled by a designated person, payments, services, goods or other economic resources provided by SolarTech Ltd to Solar SPV 2 Ltd could amount to making funds or economic resources available to a designated person. This could give rise to prohibitions, reporting obligations or the need to restrict or halt the transaction, even though Solar SPV 2 Ltd does not own the client and does not appear in the client's ownership chain.

For that reason, Operators should not limit screening only to parties shown on the main ownership chart. They should also identify and screen parties that participate in the relevant transaction, project or flow of funds, even where those parties sit elsewhere in the wider structure.

In relation to Solar SPV 1 Ltd, it will not normally be necessary to screen that entity where it is neither part of the ownership chain of the client nor involved in the transaction or project under review. On the facts given, Solar SPV 1 Ltd does not hold shares in SolarTech Ltd, does not exercise control over it and is not participating in the relevant flow of funds, goods or services. In those circumstances, it does not create an obvious sanctions exposure for the Operator in relation to the relationship with SolarTech Ltd.

However, before deciding not to screen Solar SPV 1 Ltd, the Operator should be satisfied that the entity is genuinely unrelated to the relevant transaction and does not perform any hidden operational or financing role in connection with the project. The Operator should also document the basis on which it concluded that screening Solar SPV 1 Ltd was not necessary.

In relation to the institutional investors holding limited partner interests in Green Energy Fund II, it will not normally be necessary to screen each of those investors where they hold passive interests only and do not exercise control over the fund or over SolarTech Ltd. In most fund structures, passive limited partners provide capital and receive economic returns, but do not direct the affairs of the fund, control its subsidiaries or exercise the shareholder rights attached to portfolio companies. In such circumstances, the more relevant parties for sanctions screening will usually be the fund itself and the entity exercising control over it, such as the General Partner.

That said, the Operator should remain alert to circumstances in which an investor holding a minority or limited partner interest nevertheless has governance rights, veto rights, consent rights or other contractual mechanisms capable of conferring influence over the fund or its investments. If that were the case, screening that investor may also become appropriate.

Before deciding not to screen those investors, therefore, the Operator should satisfy itself that they are genuinely passive and do not exercise ownership or control through other means. This may require review of the limited partnership agreement, side letters or other fund governance documents. The Operator should also document the basis on which it concluded that screening those investors was not necessary.

Example 3: Minority shareholders that should be screened

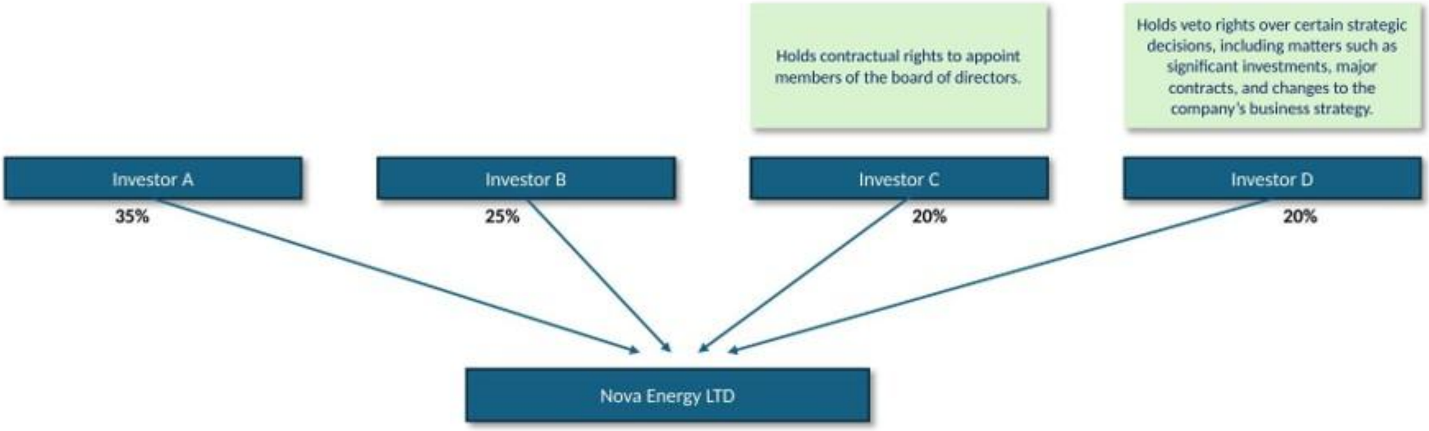
The client is Nova Energy Ltd. The ownership of Nova Energy Ltd is divided among four investors:

- Investor A – 35% shareholding
- Investor B – 25% shareholding
- Investor C – 20% shareholding
- Investor D – 20% shareholding

On the face of the shareholding percentages, none of the investors individually holds a majority interest in the company. However, the Operator has identified additional governance arrangements set out in the shareholder agreement. Under these arrangements:

- Investor C holds contractual rights to appoint members of the board of directors.
- Investor D holds veto rights over certain strategic decisions, including matters such as significant investments, major contracts, and changes to the company's business strategy.

These rights give Investors C and D the ability to influence or control the company's decision making beyond what would normally be expected from a 20 percent shareholding.



The Operator should screen the following parties:

- Nova Energy Ltd - The client should always be screened because it is the direct counterparty to the Operator. Screening the client allows the Operator to determine whether the entity itself is subject to restrictive measures.

- Investors A, B, C and D - All shareholders should be screened because they collectively represent the entire ownership structure of the client.

This is important for two reasons. Firstly, under the 50 percent ownership rule, Nova Energy Ltd would be considered owned by a designated person where one or more designated persons collectively hold 50 percent or more of the ownership interests in that entity. In this structure:

- Investor A (35%) + Investor B (25%) = 60%
- Investor A (35%) + Investor C (20%) = 55%
- Investor B (25%) + Investor C (20%) + Investor D (20%) = 65%

If two or more of these investors were designated persons, their shareholdings could aggregate to 50 percent or more, which could result in Nova Energy Ltd itself being treated as owned by designated persons. Screening all shareholders therefore enables the Operator to determine whether such aggregation may occur.

Secondly, control may arise independently of ownership thresholds. Although Investors C and D each hold only 20 percent of the shares, the shareholder agreement grants them governance rights that may enable them to exercise significant influence over the company.

Investor C holds contractual rights to appoint members of the board of directors. Through this right, Investor C may influence the composition of the company's governing body and therefore its management and strategic direction.

Investor D holds veto rights over certain strategic decisions, including significant investments, major contracts and changes to the company's business strategy. These rights allow Investor D to block key decisions of the company and therefore exert substantial influence over its activities.

Where such governance rights exist, a shareholder may be capable of exercising control or dominant influence over an entity even without holding a majority economic interest. Screening Investors C and D therefore enables the Operator to determine whether a designated person may be exercising control over the client through these governance arrangements.

If either Investor C or Investor D were identified as a designated person, the Operator should assess whether the governance rights held by that investor are capable of conferring control over Nova Energy Ltd. This assessment may require a review of the relevant corporate governance documents and, where appropriate, the Operator may seek legal advice to determine whether the rights amount to control for the purposes of sanctions compliance.

Example 4: Foundation without identifiable beneficiaries

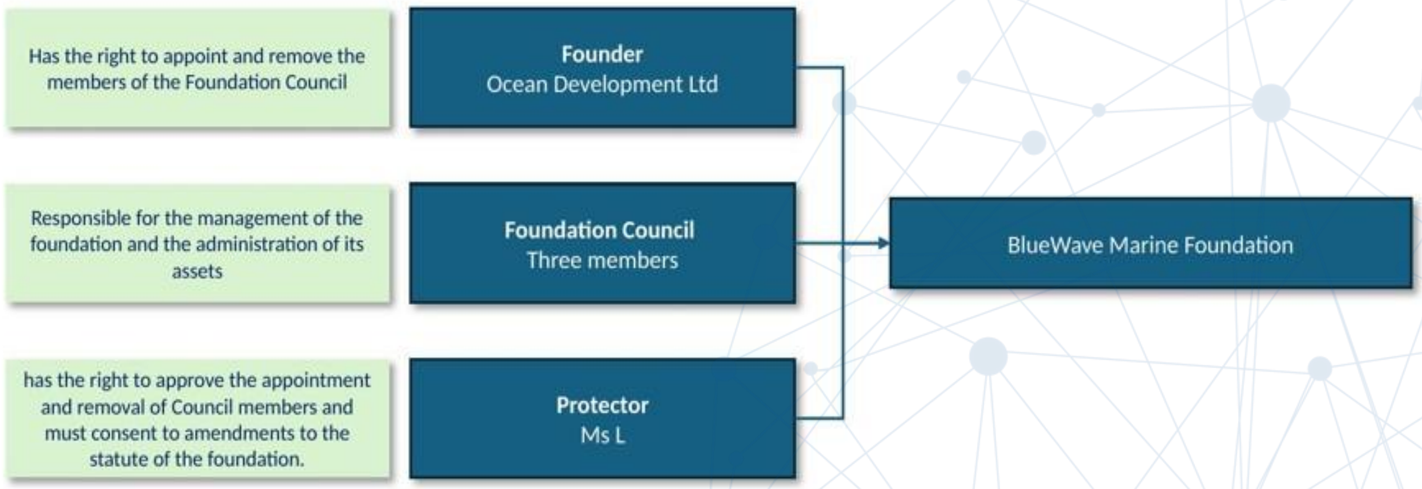
The client is BlueWave Marine Foundation, a legal entity established under a foundation structure for the purpose of supporting marine conservation projects and environmental research. The foundation has no identifiable beneficiaries. Instead, it operates for a defined purpose set out in its founding documents, namely the funding of marine conservation initiatives in coastal regions. The foundation has the following governance structure:

- Founder – Ocean Development Ltd, which has the right to appoint and remove the members of the Foundation Council.

- Foundation Council – three members responsible for the management of the foundation and the administration of its assets.

- Protector – Ms L, who has the right to approve the appointment and removal of Council members and must consent to amendments to the statute of the foundation.

The council is responsible for deciding how the foundation's funds are allocated in order to pursue its stated charitable purpose. No individual or entity has a beneficial interest in the assets of the foundation. Any distributions made by the foundation must be used exclusively for the environmental purposes defined in its statute.



In light of the information known, it would be prudent for the Operator to screen:

- BlueWave Marine Foundation - The foundation should be screened because it is the direct client.

- Ocean Development Ltd - Because, under the foundation statute, it retains the right to appoint and remove the members of the Foundation Council and to approve amendments to the statute •of the foundation. Those rights give it the ability to influence the governance of the foundation even though the foundation has no identifiable beneficiaries. Screening the founder therefore enables the Operator to determine whether a designated person may exercise control or significant influence over the foundation through these governance powers.

- Members of the Foundation Council - Because they are responsible for the administration and management of the foundation's assets. In practice, they exercise decision making authority over how the foundation's funds are used and how its purpose is pursued. If a council member were a designated person, decisions made by that person could result in funds or economic resources being made available in breach of sanctions restrictions.

- Protector - Because, under the foundation statute, she has the right to approve the appointment and removal of council members and must consent to amendments to the statute of the foundation. These rights give her the ability to exercise oversight over the governance of the foundation and to influence key decisions relating to its administration. Screening the protector therefore enables the Operator to determine whether a designated person may exercise influence or control over the foundation through these supervisory powers.

Because the foundation has no identifiable beneficiaries, the Operator should clearly determine the purpose for which the foundation was established. Understanding the purpose of the foundation is important because it allows the Operator to assess:

- the nature of the activities carried out by the foundation;

- how its funds are intended to be used; and

- whether the foundation's activities or distributions may create sanctions exposure.

For example, if the foundation makes grants or provides financial support to third parties, the Operator should consider whether those funds could ultimately be made available to a designated person.

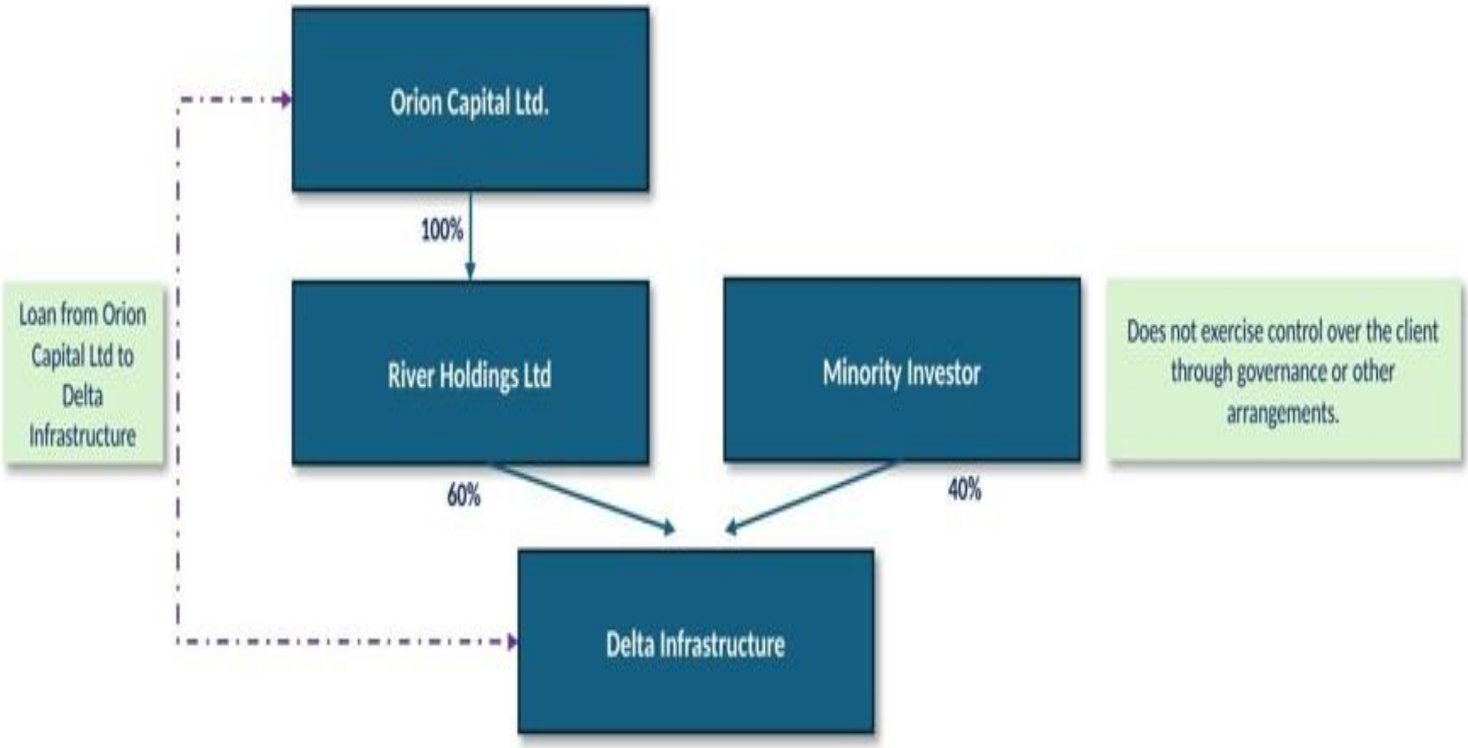
Example 5: Control arising through debt arrangements and risk through shareholding

The client is Delta Infrastructure Ltd, a project company established to develop and operate energy infrastructure assets. The ownership structure of Delta Infrastructure Ltd is as follows:

- River Holdings Ltd – 60%
- Minority Investor – 40%. The Operator has ascertained that this investor does not exercise control over the client through governance or other arrangements.

River Holdings Ltd is itself a wholly owned subsidiary of Orion Capital Ltd. Delta Infrastructure Ltd is financed through a loan facility provided by Orion Capital Ltd. The financing agreement forms part of the company's initial funding structure. Under the financing agreement:

- Orion Capital Ltd has provided a substantial loan facility to Delta Infrastructure Ltd.
- Delta Infrastructure Ltd may not incur additional debt, dispose of material assets, approve major investments or amend its business plan without the consent of Orion Capital Ltd.
- Orion Capital Ltd has the right to appoint a board observer and receives regular financial and operational reporting from the company.
- Orion Capital Ltd does not hold shares in Delta Infrastructure Ltd.



In light of the information known, it would be prudent for the Operator to screen:

- Delta Infrastructure Ltd - The client should always be screened because it is the direct counterparty to the Operator. Screening the client allows the Operator to determine whether the entity itself is subject to restrictive measures.

- River Holdings Ltd - Because it holds a controlling ownership interest in the client. Screening the parent entity enables the Operator to determine whether the client may be owned or controlled, directly or indirectly, by a designated person.

- Orion Capital Ltd - Although Orion Capital Ltd does not hold shares in Delta Infrastructure Ltd directly, it should also be screened because it provides financing to the company and holds contractual rights capable of influencing the company's activities. Through the financing agreement, Orion Capital Ltd has the ability to restrict additional borrowing, approve major investments and influence the company's business plan. These rights may enable Orion Capital Ltd to exercise significant influence over the financial and strategic direction of the company.

If Orion Capital Ltd were identified as a designated person, the Operator would need to assess whether the rights arising under the financing arrangements are capable of conferring control over Delta Infrastructure Ltd, for the purposes of sanctions compliance. In practice, the Operator would typically consider, inter alia:

- the scope of the lender consent rights;
- the extent of governance influence;
- step-in or enforcement rights (e.g. the right to take control of the company's operations following a default, the right to appoint administrators or replacement management, the right to assume control of key assets);
- the practical dependency of the company on the financing (if the loan facility represents the company's primary source of funding and cannot realistically be replaced, the lender may have substantial leverage over the company's decisions); and
- the overall effect of the rights.

If the review indicates that Orion Capital Ltd is able to determine or block the company's strategic or financial decisions, the Operator may conclude that the lender is capable of exercising control or dominant influence over Delta Infrastructure Ltd. In practice, this assessment would normally involve reviewing the loan agreement, shareholder agreements and constitutional documents of the company, and where the position is unclear the Operator may seek legal advice to determine whether the rights amount to control for the purposes of sanctions compliance.

In relation to the Minority Investor, were they to be found to be a designated entity, the 50 percent ownership rule would not be triggered, because the shareholder holds only 40 percent. The client would also not automatically be considered controlled by the designated person, because we have established that the shareholder does not exercise control. Therefore, the client itself would not become a sanctioned entity. The Operator could still face sanctions exposure if funds or economic resources are made available to that shareholder.

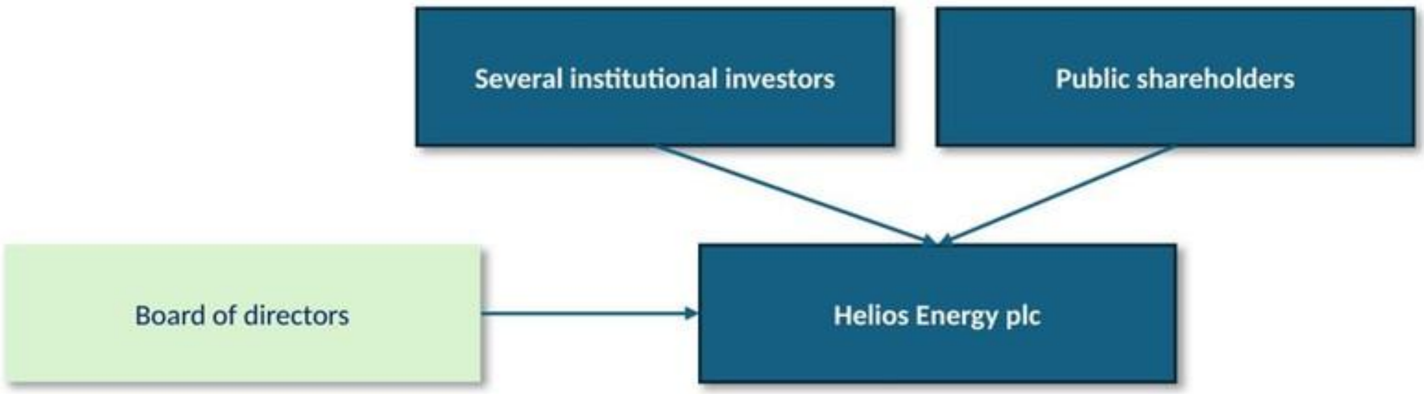
In determining whether the Minority Investor should be screened, the Operator should adopt a risk-based and proportionate approach. In this case, where the shareholding is held by a single identifiable investor, the Operator may consider that screening the shareholder is straightforward and proportionate. By contrast, where ownership interests are dispersed among a large number of small passive investors, such as in a fund with hundreds of limited partners or a company with a very large shareholder base, screening every individual investor may not be proportionate to the risk, particularly where those investors hold small passive interests, do not exercise governance rights and cannot exercise control or reach the relevant ownership thresholds.

Example 6: Client that is a company listed on a stock exchange

The client is Helios Energy plc, a company listed on a regulated stock exchange within the European Economic Area. The company's shares are publicly traded, and ownership is widely distributed among a large number of investors. The Operator understands, based on publicly available information and corporate disclosures, that no shareholder holds a controlling interest in the company. The company's governance structure includes:

- a board of directors responsible for the management and strategic direction of the company;
- several institutional investors, each holding small minority interests; and
- public shareholders, whose shares are traded on the stock exchange.

Because Helios Energy plc is listed on a regulated market, its shareholders change frequently through trading activity, and individual shareholders may not be readily identifiable.



In light of the information known, it would be prudent for the Operator to screen:

- Helios Energy plc - The client should always be screened because it is the direct counterparty to the Operator. Screening the client allows the Operator to determine whether the company itself is subject to restrictive measures.

- Members of the Board of Directors - The members of the board should be screened because they are responsible for the management and strategic direction of the company. Screening them allows the Operator to determine whether a designated person may exercise influence over the company through its governing body.

In relation to shareholders of the listed company, it will not normally be necessary for the Operator to identify and screen all shareholders of a company whose shares are admitted to trading on a regulated market within the European Economic Area. This is because:

- Ownership of listed companies is typically widely distributed and changes frequently through market trading;
- Individual shareholders may not be readily identifiable; and
- The Operator does not generally make funds or economic resources available directly to those shareholders.

Instead, the Operator should confirm that the company is listed on a regulated market subject to appropriate disclosure requirements, and should review publicly available information to determine whether any shareholder has disclosed a significant or controlling interest. If publicly available information indicates that a particular shareholder holds a significant ownership interest or exercises control over the company, the Operator should consider whether screening that shareholder would also be appropriate.

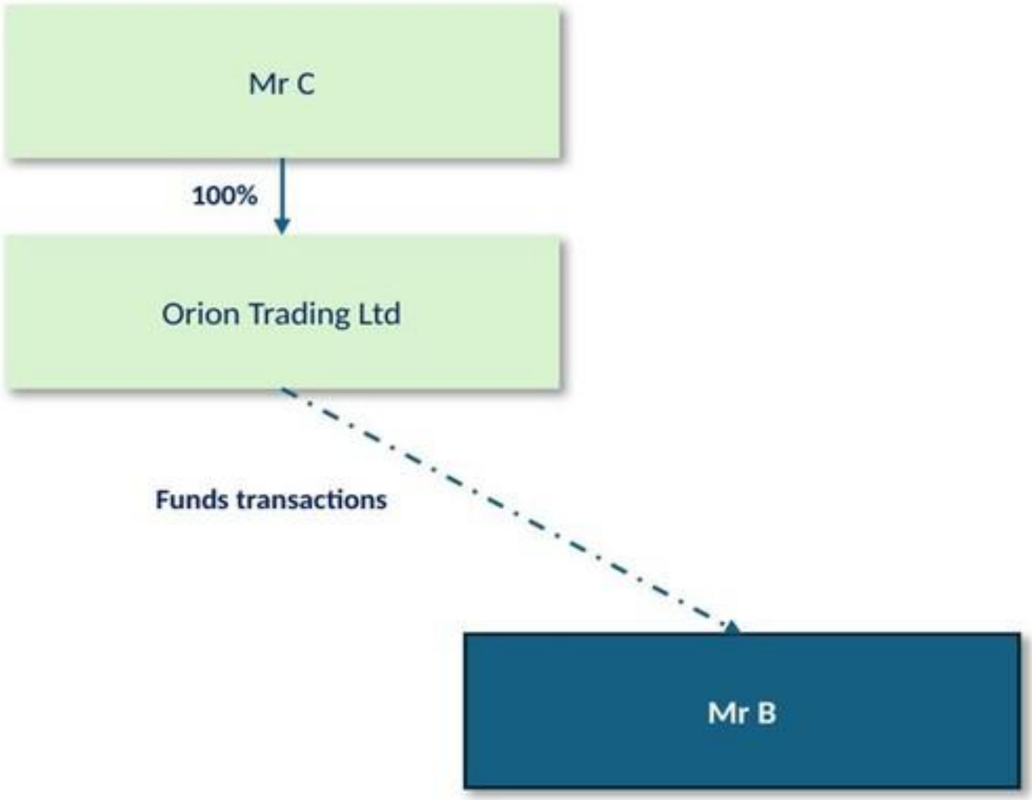
Example 7: Risk of sanctions circumvention through the use of a gambling nominee account

The Operator is LuckySpin Gaming Ltd, an online gambling operator. The client is Mr B, an individual who opens an account with LuckySpin. Mr B states that he intends to place wagers on sporting events and casino games. During onboarding he indicates that he will fund the account through bank transfers from his personal account.

Shortly after the account is opened, however, the Operator observes that the funds used to finance the gambling activity do not originate from Mr B’s personal bank account. Instead, deposits are received from Orion Trading Ltd, a company incorporated in Cyprus. Over a period of several weeks:

- Orion Trading Ltd makes multiple deposits into Mr B’s gambling account;
- Mr B places wagers using the account; and
- A portion of the winnings is withdrawn to accounts held by Orion Trading Ltd.

The Operator conducts further enquiries and establishes that Mr C is the beneficial owner of Orion Trading Ltd. The structure of the arrangement is therefore as follows: Mr C is the beneficial owner of Orion Trading Ltd; Orion Trading Ltd transfers funds to the gambling account; and Mr B is the account holder placing wagers. Funds flow from Orion Trading Ltd to Mr B's gambling account, Mr B places bets, and withdrawals are subsequently made to accounts held by Orion Trading Ltd.



In light of the information known, it would be prudent for the Operator to screen, at onboarding:

- Mr B - The client should always be screened because it is the direct counterparty to the Operator. Screening the client allows the Operator to determine whether the company itself is subject to restrictive measures.

Upon identification of the transactional pattern:

- Orion Ltd Trading - Orion Trading Ltd should also be screened because it is the entity providing the funds used to finance the gambling activity. Although Orion Trading Ltd is not the account holder, it participates directly in the financial flows associated with the relationship. If Orion Trading Ltd were a designated person, accepting deposits from that entity could amount to dealing with frozen funds or making economic resources available to a designated person.

- Mr. C - Mr. C should also be screened because he is the beneficial owner of Orion Trading Ltd. If Orion Trading Ltd were owned or controlled by a designated person, the Operator could be indirectly dealing with funds belonging to that designated person.

The pattern observed creates a potential risk that the account held by Mr B is being used on behalf of another person. If Mr C were a designated person, this arrangement could allow him to access gambling services and move funds through the Operator indirectly. In such circumstances, the Operator could be making funds or economic resources available, directly or indirectly, to a designated person, even though the gambling account itself is held in the name of Mr B.

Example 8: Affiliate marketing partner

The Operator is LuckySpin Gaming Ltd, an online gambling operator. LuckySpin Gaming entered into a commercial relationship with BetBoost Media Ltd, a digital marketing company that operates gambling affiliate websites. BetBoost Media Ltd promotes LuckySpin Gaming Ltd through online advertising, comparison websites and referral links. Under the affiliate agreement:

- BetBoost promotes LuckySpin through its websites and marketing channels;

- Players who register with LuckySpin through BetBoost referral links are tracked through affiliate software; and

- BetBoost receives a revenue share commission calculated as a percentage of the net gambling revenue generated by those referred players.

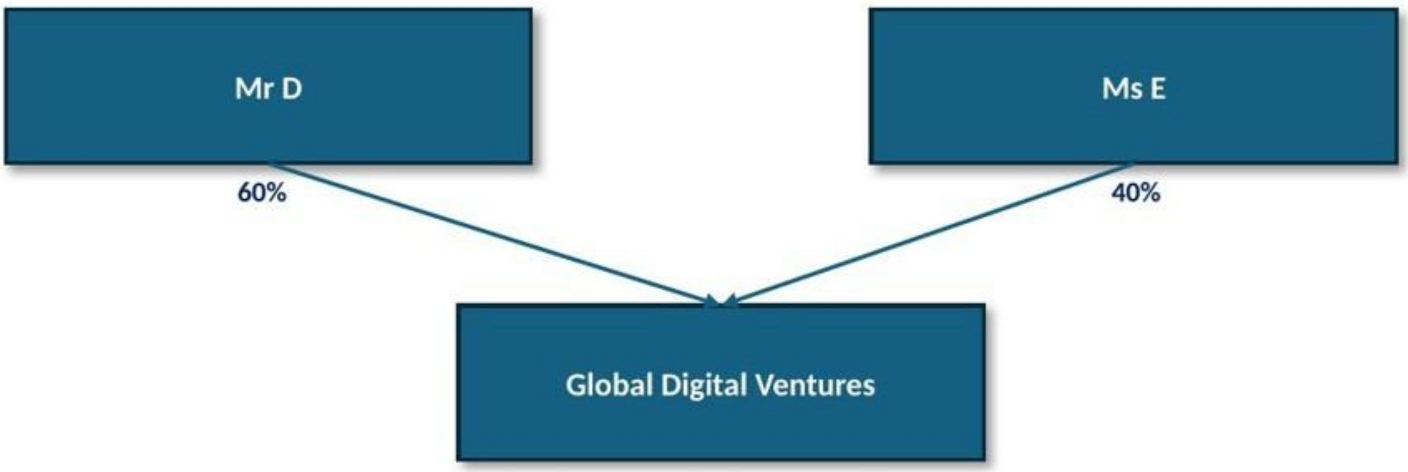
The Operator identifies that BetBoost is wholly owned by Global Digital Ventures Ltd, a holding company incorporated in the United Arab Emirates. Global Digital Ventures Ltd has the following ownership structure: Mr. D – 60% shareholding; Ms. E – 40% shareholding. On the face of the ownership percentages, Mr. D appears to hold the controlling interest. However, the Operator reviews the shareholder agreement and corporate governance arrangements and identifies the following provisions:

- Ms. E has the right to appoint two of the three directors of Global Digital Ventures Ltd;

- The board of directors is responsible for approving the commercial strategy of the company, including affiliate marketing agreements; and

- Certain key decisions, including entry into affiliate partnerships, approval of marketing budgets and distribution of profits, require the approval of Ms E under the shareholder agreement.

As a result of these governance arrangements, Ms E is able to direct the strategic and commercial decisions of the company, including decisions relating to the operation of BetBoost Media Ltd.



In light of the information known, it would be prudent for the Operator to screen:

- BetBoost Media Ltd - BetBoost Media Ltd should be screened because it is the direct contractual counterparty of the Operator and receives commission payments under the affiliate agreement. If BetBoost Media Ltd were a designated entity, paying commission to it would amount to making funds available to a designated person.

- Global Digital Ventures Ltd - Global Digital Ventures Ltd should also be screened because it owns BetBoost Media Ltd. If Global Digital Ventures Ltd were owned or controlled by a designated person, BetBoost Media Ltd could also be considered owned or controlled by a designated person through the ownership chain.

- Mr D - Should be screened because he holds a significant ownership interest in Global Digital Ventures Ltd. Were he to be a designated entity, the 50% rule would be triggered.

In relation to Ms E, she should be screened because she exercises control over Global Digital Ventures Ltd through governance rights, even though she holds only a minority shareholding. If Ms E were a designated person, Global Digital Ventures Ltd could be considered controlled by a designated person, and BetBoost Media Ltd, as its wholly owned subsidiary, could also be considered controlled by a designated person. In that situation, payments made by the Operator to BetBoost Media Ltd could amount to making funds or economic resources available to a designated person

Example 9: Aggregation of ownership interests held by designated persons across different levels of the structure

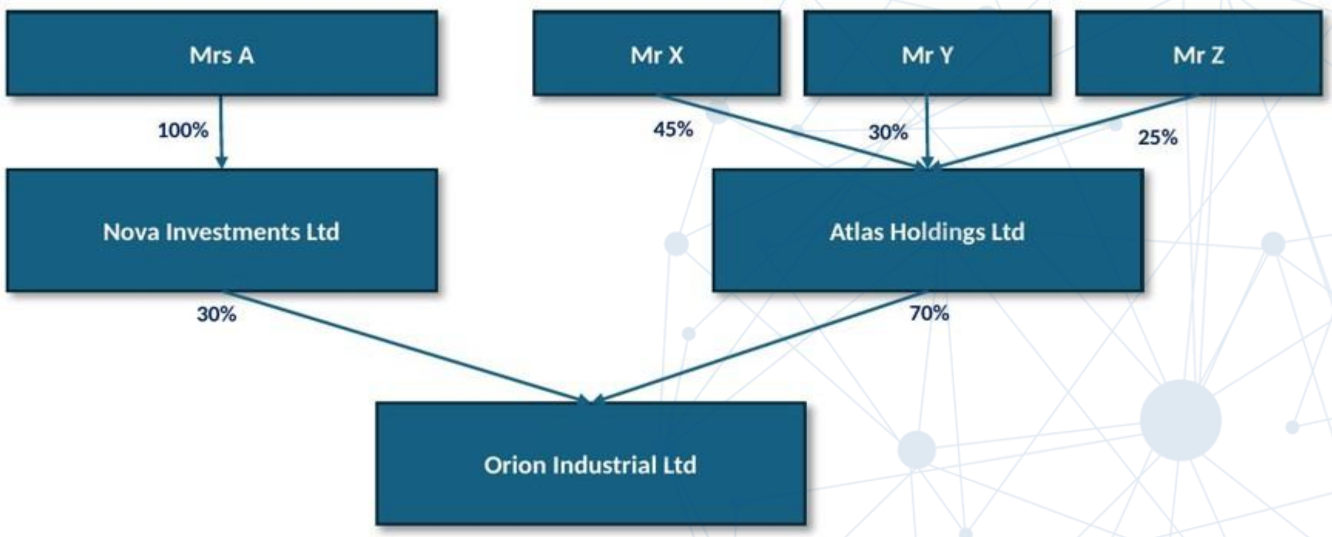
The client is Orion Industrial Ltd, a company incorporated in Malta. The ownership structure of Orion Industrial Ltd is as follows:

- Atlas Holdings Ltd – 70%
- Nova Investments Ltd – 30%

The Operator establishes that Nova Investments Ltd does not exercise control over the client through governance or other arrangements. Atlas Holdings Ltd is itself owned as follows:

- Mr X – 45%
- Mr Y – 30%
- Mr Z – 25%

Nova Investments Ltd is 100% owned by Mrs A. The Operator reviews the shareholder agreement and confirms that no single shareholder has unilateral control over Atlas Holdings Ltd; decisions are taken by simple majority; and no shareholder holds veto rights or special governance rights capable of conferring control individually.



In light of the information known, it would be prudent for the Operator to screen:

- Orion Industrial Ltd - The client should always be screened because it is the direct counterparty to the Operator.

- Atlas Holdings Ltd - Because it holds a controlling ownership interest (70%) in the client. Screening the parent entity allows the Operator to determine whether the client may be owned or controlled by a designated person through the ownership chain.

- Nova Investments Ltd - Because it is a direct shareholder of the client and may receive distributions or other economic resources. Even though it holds only 30%, if it were a designated person, payments such as dividends could amount to making funds available to a designated person.

- Mr X, Mr Y and Mr Z - Because they collectively represent the ownership of the entity that controls the client and sanctions exposure may arise through the aggregation of ownership interests held by designated persons.

- Mrs A - As the owner of Nova Investments Ltd.

The Operator identifies that Nova Investments Ltd (30%) is a designated entity, and Mr Z (25%), a shareholder of Atlas Holdings Ltd, is also a designated person. The Operator should consider how these interests translate into ownership of the client.

In terms of direct ownership, Nova Investments Ltd holds 30% of Orion Industrial Ltd, and the 50% ownership threshold is not met through Nova Investments Ltd alone. In terms of indirect ownership, Mr Z holds 25% of Atlas Holdings Ltd, which in turn holds 70% of Orion Industrial Ltd. This results in an indirect ownership interest of 25% × 70% = 17.5% in Orion Industrial Ltd.
The Operator should aggregate ownership interests held by designated persons at the level of the client. In this case: Nova Investments Ltd 30% (direct) plus Mr Z 17.5% (indirect through Atlas Holdings Ltd). Total designated ownership: 47.5% of Orion Industrial Ltd.

Because the aggregate ownership held by designated persons is below 50%, Orion Industrial Ltd would not automatically be considered owned by designated persons under the ownership test. However, the presence of designated persons holding a significant combined interest creates elevated sanctions risk, and the Operator must ensure that it does not make funds or economic resources available to those designated persons. In particular, any distributions to Nova Investments Ltd would be prohibited, and the Operator should consider whether any flows of value could indirectly benefit Mr Z. In these circumstances, the Operator should consider whether safeguards can be implemented to prevent such flows, and where such safeguards cannot be implemented, should consider restricting or declining the relationship.

Even where the 50% ownership threshold is not met, the Operator should assess whether control may arise through other means and should consider whether there are arrangements between shareholders that could enable coordinated action or influence. For example, if Nova Investments Ltd and Mr Z were acting together, or governance arrangements allowed them to influence decisions jointly, the Operator may need to assess whether control or dominant influence could arise notwithstanding the ownership percentages.

Example 10: Aggregation involving parties designated under different sanctions regimes

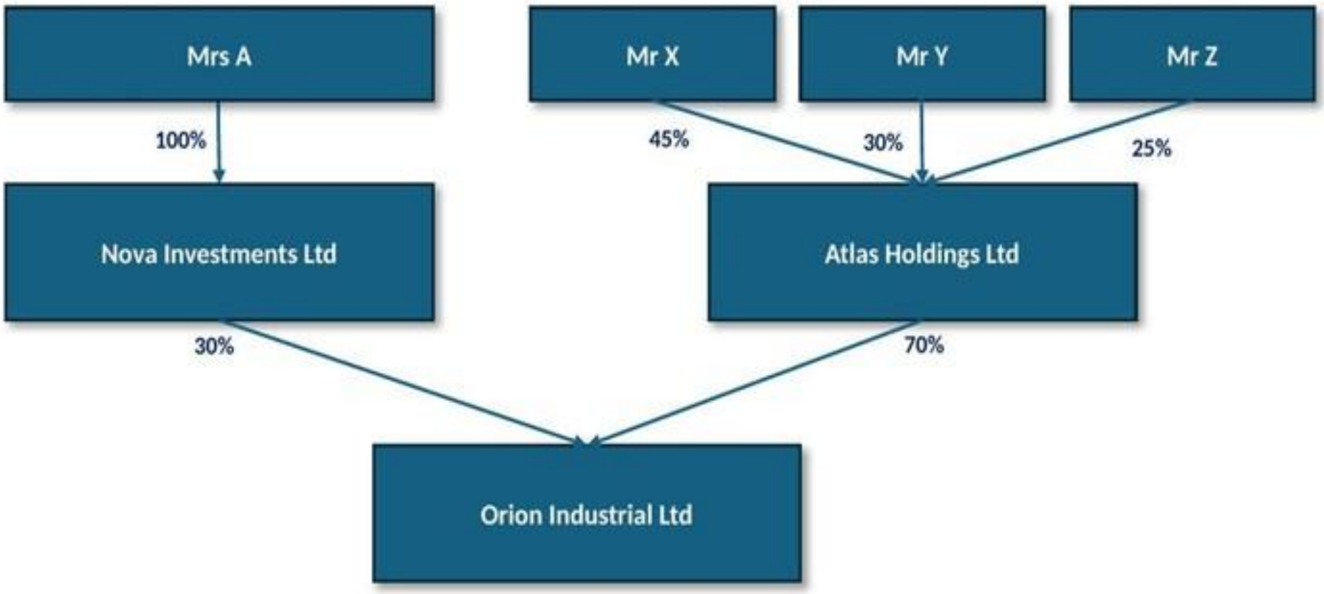
The client is Orion Industrial Ltd, a company incorporated in Malta. The ownership structure of Orion Industrial Ltd is as follows:

- Atlas Holdings Ltd – 70%
- Nova Investments Ltd – 30%

The Operator establishes that Nova Investments Ltd does not exercise control over the client through governance or other arrangements. Atlas Holdings Ltd is itself owned as follows:

- Mr X – 45%
- Mr Y – 30%
- Mr Z – 25%

Nova Investments Ltd is 100% owned by Mrs A. The Operator reviews the shareholder agreement and confirms that no single shareholder has unilateral control over Atlas Holdings Ltd; decisions are taken by simple majority; and no shareholder holds veto rights or special governance rights capable of conferring control individually.



In light of the information known, it would be prudent for the Operator to screen:

- Orion Industrial Ltd - The client should always be screened because it is the direct counterparty to the Operator.

- Atlas Holdings Ltd - Because it holds a controlling ownership interest (70%) in the client. Screening the parent entity allows the Operator to determine whether the client may be owned or controlled by a designated person through the ownership chain.

- Nova Investments Ltd - Because it is a direct shareholder of the client and may receive distributions or other economic resources. Even though it holds only 30%, if it were a designated person, payments such as dividends could amount to making funds available to a designated person.

- Mr. X, Mr. Y and Mr. Z - Because they collectively represent the ownership of the entity that controls the client and sanctions exposure may arise through the aggregation of ownership interests held by designated persons.

- Mrs. A - As the owner of Nova Investments Ltd.

The Operator identifies that Nova Investments Ltd (30%) is a designated entity under EU restrictive measures, and Mr. Z (25%), a shareholder of Atlas Holdings Ltd, is designated under US OFAC sanctions. For the purposes of EU sanctions, aggregation is performed only in respect of designated persons under EU restrictive measures. In this case, therefore, Mr Z (OFAC designated only) not counted for EU aggregation.

This means that the 50% ownership threshold for Orion Industrial Ltd is not met and it is not considered controlled by a designated person. That notwithstanding, the Operator must ensure that it does not make funds or economic resources available to Nova Investments Ltd, and any distributions or payments to that entity would be prohibited. The relationship with Orion Industrial Ltd may still be possible, provided that the Operator can ensure that its services do not result in funds being made available to Nova Investments Ltd, and no other sanctions prohibitions are triggered.

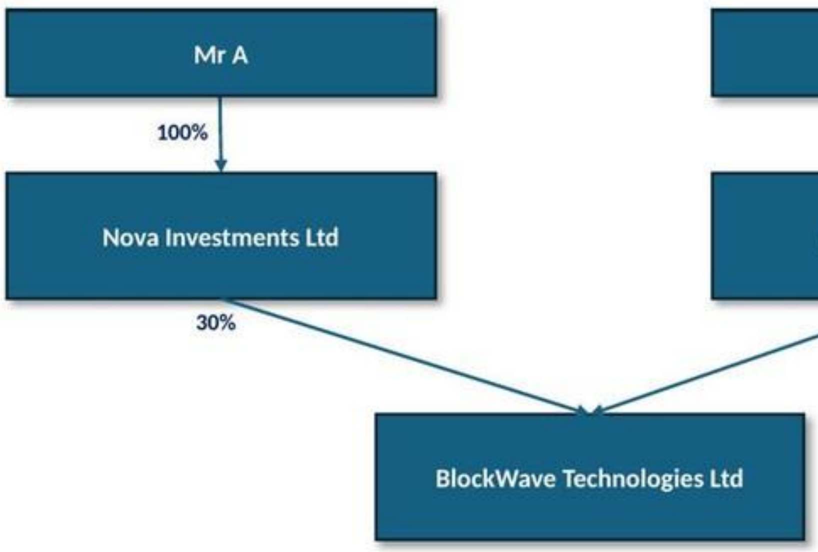
In relation to Mr Z, although he is not designated under EU sanctions, his designation under OFAC may still be relevant. In particular, the Operator should consider whether it has US nexus exposure (for example, use of US dollars, US financial institutions, or US operations); if such a nexus exists, OFAC restrictions may become applicable and it would be prudent for the Operator to consider, inter alia, exposure to the risk of secondary sanctions. Even where no direct legal obligation arises, the Operator may consider reputational, commercial or correspondent banking risks associated with dealing with an OFAC-designated individual.

Example 11: Aggregation involving parties designated under different sanctions regimes

The client is BlockWave Technologies Ltd, a company incorporated in an EU Member State. BlockWave Technologies Ltd approaches the Operator (a CASP) to open a corporate account, and to access services including custody and fiat on/off-ramp for its treasury and operational crypto-assets. The ownership structure of BlockWave Technologies Ltd is as follows:

- Alpha Ventures Ltd – 70%
- Nova Investments Ltd – 30%

Alpha Ventures Ltd and Nova Investments Ltd are respectively owned by Mr A (100%) and Mr B (100%); they are also both signatories of BlockWave Technologies Ltd.



In light of the information known, it would be prudent for the Operator to screen:

- BlockWave Technologies Ltd - The client should always be screened as the direct counterparty.
- Alpha Ventures Ltd - Because it holds a majority ownership interest and may exercise control over the client.

- Nova Investments Ltd - Because it is a direct shareholder and may receive funds or economic resources.

- Mr A and Mr B - As the beneficial owners and authorised signatories of Alpha Ventures Ltd, Nova Investments Ltd and BlockWave Technologies Ltd. Directors and wallet signatories should be screened because they may control the use of crypto-assets and the execution of transactions.

Screening identifies that Nova Investments Ltd (30%) is a designated entity under EU restrictive measures. No other shareholders or controllers are identified as designated persons. In this case, the 50% ownership threshold is not met and BlockWave Technologies Ltd is therefore not deemed to be owned or controlled by a designated person. However, as Nova Investments Ltd is a designated entity, making funds or economic resources available to it is prohibited.

Because BlockWave Technologies Ltd intends to receive crypto-assets into hosted wallets provided by the Operator, convert crypto-assets into fiat, and periodically distribute profits to its shareholders, the Operator identifies that crypto-assets held in custody form part of the client's economic resources, and increases in value of those assets may ultimately benefit shareholders. Distributions may occur either in fiat or directly in crypto-assets to external wallets. In other words, transfers of crypto-assets to wallets controlled by Nova Investments Ltd would constitute making economic resources available to a designated entity. In addition, the fungible and transferable nature of crypto-assets increases the risk that value may be transferred quickly and with limited visibility once assets leave the Operator's environment.

In these circumstances, the Operator should assess whether it can ensure that its services do not result in funds or economic resources being made available to Nova Investments Ltd. This may include:

- determining whether distributions to shareholders can be restricted or prohibited;

- assessing whether wallet-level controls can prevent transfers to addresses associated with Nova Investments Ltd;

- considering whether governance arrangements allow the Operator to rely on the client to enforce such restrictions; and

- evaluating whether the client's business model inherently involves flows of value to shareholders.

Where the Operator can implement effective measures to ensure that no funds or economic resources are made available, directly or indirectly, to Nova Investments Ltd, the relationship may be possible. Where the Operator cannot ensure this, for example because distributions are integral to the business model or crypto-assets may be transferred to external wallets beyond the Operator's control, the Operator should not establish or should terminate the relationship.

For any queries regarding this document, please contact us at sanctions.smb@gov.mt.

Sanctions Monitoring Board, 2026
Website: www.smb.gov.mt

SMB
BORD TA' SORVELJANZA DWAR IS-SANZJONIJIET
SANCTIONS MONITORING BOARD
MALTA