Guidance note on the application of Article 17(6)(a),(b) and (c) of the National Interest (Enabling Powers) Act.

This guidance note is produced by the Sanctions Monitoring Board (**SMB**) as the competent authority for the implementation of financial sanctions in the Republic of Malta in pursuance of its power under Article 7(5)(b) of the National Interest (Enabling Powers) Act.

The SMB's website is: https://foreignaffairs.gov.mt/SMB and the SMB may be contacted at: sanctions.mftp@gov.mt

November 2019

I. Introduction

Further to the Guidance Note issued in October 2019 on 'Targeted Financial Sanctions' in Malta, the SMB would like to draw the attention of all subject persons on the requirements of Article 17(6)(a), (b), and (c) of the National Interest (Enabling Powers) Act, Cap 365 of the Laws of Malta, reproduced hereunder, particularly the requirement to have in place and effectively implement internal controls and procedures to ensure compliance with applicable sanctions at all times.

"Any legal or natural person conducting a relevant activity or relevant financial business as defined in the Prevention of Money Laundering Act shall be required to:

> *(a) regularly check the list of designations by the UN, the EU, and the Sanctions Board, and to screen their client databases against those lists on a regular basis and immediately after a change to any of these lists occurs;*
>
> *(b) have in place and effectively implement internal controls and procedures to ensure compliance with the obligations arising from this Act and any relevant UN or EU Resolutions or Regulations; and*
>
> *(c) immediately notify the Board in case targeted property is identified, and of the actions taken in relation to such property in compliance with the requirements under this Act, including in relation to any attempted transactions."*

II. Internal Controls and Procedures

Article 17(6)(b) of the National Interest (Enabling Powers) Act requires that subject persons have systems in place. The objective behind this legal obligation is to ensure that the aims for which EU and UN restrictive measures would have been put in place, are effectively achieved.

Internal controls and procedures which subject persons are required to have must be adequate and effective in order to achieve the required result, as described under Article 17(6). The processes and procedures followed by the subject person should enable the flagging of hits from within its client list with sanctioned persons or entities. It should also enable subject persons to regularly monitor their customers as required under Article 17(6)(a). Subject persons must employ sanctions screening processes that are proportionate to the nature and size of the subject person's business, based on the subject person's self-assessment of needs and risk of being in breach of applicable sanctions, in order to detect whether potential and current customers or other entities and individuals involved in the structure, are subject to UN, EU or national sanctions. When conducting its self-assessment, a subject person should take into account:

- Its activities, products and client base;
- Channels of distribution;
- Complexity, frequency and volume of transactions;

- Its processes, systems and their respective parameters;
- Operating environment;
- Screening processes of other entities within a group of companies;
- Geographical risk related to where the client conducts its business and generates its proceeds; and
- Other risk factors which the subject persons may be exposed to, including industry-specific risk factors

The adoption of internal controls and procedures is necessary on all subject persons in order to ensure that any potential sanctions violation is prevented and detected in an efficient and effective manner. Effective controls and procedures include, but are not limited to, ensuring that company personnel involved in compliance are trained and kept updated with sanctions screening obligations, having written procedures which lay down the course of action to be taken in case of a hit and updating or changing the systems used for sanctions screening when this is no longer proportionate to the size or complexity of the business. Breaches of sanctions, such as the provision of corporate or accounting services to a sanctioned individual or entity or the registration of a contract of sale which involves a sanctioned individual or entity, even inadvertently, entail heavy penalties as envisaged under Article 6 of the National Interest (Enabling Powers) Act:

a) Imprisonment for a term of twelve months to twelve years or a fine (multa) of not less than EUR 25,0000 and not more than EUR 5,000,000 or to both imprisonment and fine;
b) Where the offence is committed by a body corporate, a fine (multa) of not less than EUR 80,000 and not more than EUR 10,000,000;
c) Where the offence by the body corporate is committed as a result of the lack of supervision or control of the director, manager, company secretary or other principal officer, such person shall also be liable for the punishment in (b);
d) Where the offender is a body corporate, the court may also impose:
    - The suspension or cancellation of any license, permit or other authority to engage in any trade, business or other commercial activity;
    - The temporary or permanent closure of any establishment used for the commission of the offence;
    - The compulsory winding up of the body corporate;
    - Exclusion from entitlement to public benefits or aid.
e) The directors, company secretary and manager or other officer of a body corporate found to be guilty of an offence under (b) or (c), shall also be guilty of an offence unless they prove that the offence was committed without their knowledge and that they exercised all due diligence to prevent the commission of the offence

Moreover, it is recommended that subject persons update the internal controls and procedures in line with guidance notes issued by the SMB.

III. Sanction Screening Systems, Software and Processes

Multiple firms may use automated screening software whilst others rely on other systems such as manual screening. The scope and complexity should ultimately depend on the subject person's business activities and business profile. Subject persons are to consider what type of screening systems or software is to be utilised in accordance with the nature, volume, frequency, complexity and risk profiles of their business and clientele. The key element in determining the adequacy of the screening method used is that the system in place flags hits clearly and promptly. Although the consolidated lists of UN[1]

[1] UN Security Council consolidated list can be found at https://www.un.org/securitycouncil/content/un-sc-consolidated-list

and EU[2] sanctions are readily available, the effectiveness of manual online checks from the aforementioned lists fundamentally remain dependent on the nature, number of clients and complexity of business relations.

It is imperative that checks are made on all client databases prior to the onset of an occasional transaction or a business relationship and at regular intervals thereafter. In the case of customers with which a business relationship is created, the frequency of checks depends on the risk which that customer poses, the internal processes and procedures which the subject person has adopted and also the type of transaction involved. In the case of established business relationships with clients that are body corporates, the screening process should be repeated every time there is a change in the beneficial ownership. Firms are to ensure that their screening process is reviewed and updated periodically and in particular, upon the occurrence of trigger events, to reflect key changes made to the sanctions regime, such as the addition of new jurisdictions or regimes. The effectiveness of systems used, whether automated or manual should be monitored and automated systems should be tested periodically to ensure they are working as intended.

In this regard, regular checks need to be made to ensure that no business is conducted with a listed person or entity whether directly or indirectly and regardless of the value of the transactions or the amount of funds involved. This applies both to occasional transactions and also to transactions which take place within the context of an ongoing business relationship. It also applies to client accounts that are deemed to be dormant.

Sanctions screening is also required in relation to other entities or individuals which may be involved in the client's ownership and control structures. This entails that the structure behind legal entities is examined as part of the due diligence process. In this regard, the subject person needs to ascertain that no sanctions have been imposed on beneficial owners and other natural or legal persons that exercise control within the structure, such as directors and trustees, as defined under the Prevention of Money Laundering and Funding of Terrorism Regulations and the Implementing Procedures, and other persons that exercise control through other means such as through voting rights. Checks must also be made to ascertain that the transaction itself does not violate applicable sanctions, even though no listed persons or entities might be involved, such as a transaction which involves the importation or exportation of a prohibited item.

For businesses involving a sizeable client database, large volumes and complex transactions, sole reliance on manual sanction checks is not deemed a viable option in terms of effectiveness and in compliance with article 17(6)(b) of the National Interest (Enabling Powers) Act. Specialised software needs to be put in place to provide an instant, efficient and reliable method of ensuring the required level of screening.

IV. Outsourcing

Outsourcing refers to the delegation of the obligations which emanate from Article 17(6) of the National Interest (Enabling Powers) Act. The third party to whom sanctions screening is outsourced must follow procedures which meet the level of effectiveness required from the subject person. However, the subject person will remain fully responsible to fulfil the obligations under the National Interest (Enabling Powers) Act and the fact of outsourcing will not exempt the subject person from liability in case of a sanctions breach. In fact, if there is a hit, the responsibility of informing the Sanctions Monitoring Board remains with the subject person, even if the actual screening would have been carried out by a third party. Thus, the subject person must ensure that there is a process of communication between the subject person and the contracted person, which facilitates exchange of information in case of a hit. Outsourcing is to be distinguished from reliance by the subject person on checks carried out by a third party who would have carried out the checks to meet its own legal obligations. Where a new client is

[2] https://data.europa.eu/euodp/en/data/dataset/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions and https://www.sanctionsmap.eu/#/main

onboarded or taken over from another subject person, it should not be assumed that screening has already taken place and independent checks need to be done to satisfy screening obligations.

V. Record Keeping

It is furthermore necessary that all client files screened via automated or manual systems contain evidence which proves that the required sanctions checks have been made prior to the start of the business relationship and periodically thereafter or at the onset of an occasional transaction. Records of sanctions checks should be retained in order to show that the subject person effectively discharged its obligations at law.

Whether firms screen using automated systems or manually, a dated audit trail of checks undertaken should be retained. In terms of good practice, records of checks should be filed, whether electronically or in hard copy, for a period of no less than five years, commencing from the date of termination of the business relationship or the fulfilment of the occasional transaction. Records should be kept with the subject person even when sanction screening is outsourced. Filed evidence of checks which are dated a few days prior to a compliance examination carried out by the FIAU, the MFSA or the MGA, as supervisory authorities and agents of the SMB, will not be considered as satisfying the requirements of article 17(6)(a) and (b) of the National Interest (Enabling Powers) Act.

The Sanctions Monitoring Board hereby encourages all subject persons to ensure that client files are kept updated and under review at all times.

VI. Staff Training

All subject persons need to ensure that staff involved in the compliance process are aware, fully understand and are properly trained on the importance and use of sanctions screening procedures and ensure that these processes are used at all times. This also entails a proper knowledge of what sanctions are, what they try to achieve and an awareness of potential cases of sanction circumvention in order that these may be properly detected.

Staff must also be made aware of typical approaches which sanctioned parties may use to evade detection of their illicit activities such as structuring transactions with the purpose of concealing the involvement of a sanctioned party. In this regard, an awareness of 'fuzzy matching' would also be essential in order for checks to be done on variations of the names or in case of misspelt, incomplete or missing information.

Any changes in procedures or sanctions requirements likewise need to be communicated to staff in good time. Staff also need to be aware of what needs to be done in case a potential sanctions issue is encountered.

VII. 'Tipping Off'

Tipping off refers to the disclosure of information to the applicant for business about the actions taken by the subject person following a hit. Subject persons are prohibited from informing a customer or any third party of a potential sanctions breach as this would constitute tipping off in terms of Article 17(7) of the NIA. Once disclosure of information takes place, this would constitute tipping off even if the investigation by the Sanctions Monitoring Board is not actually prejudiced. It is therefore important that all those employees who are client-facing, know of the obligation not to tip off. In case of doubt as to whether the hit constitutes a false positive or not, the subject person must refrain from communicating this to the client before obtaining the approval of the SMB in writing.

VIII. Submission of Information

The SMB must be informed immediately in case of a hit and of the measures taken by the subject person. Failure to do so constitutes an offence. Should any situation be encountered which is in violation of sanctions, whether directly or indirectly, there is an obligation to stop any transaction from going through, freeze any assets and inform the SMB. In practice this also means that the subject person must not deal with such assets or make them available to, directly or indirectly, or for the benefit of, the sanctioned person. This also carries with it an obligation not to 'tip off' the listed person. Communication with the SMB should be made effected without delay and via email or in writing on the contact details provided on the SMB webpage which can be accessed here: https://foreignaffairs.gov.mt/en/Government/SMB/Pages/Sanctions-Monitoring-Board.aspx
Supporting documentation, such as documents which identify the sanctioned person, should also be provided to the SMB.

The SMB remains at the disposition of the subject person in case any further information or clarifications are required. The Board may be contacted on sanctions.mftp@gov.mt. Reference may also be made to section 4.11 of the Implementing Procedures issued by the Financial Intelligence Analysis Unit, for further guidance.

Subject persons are invited to subscribe to the mailing list of the SMB by sending an email on sanctions.mftp@gov.mt in order to receive regular updates related to sanctions.