

The section on the Sanctions Act in the former DNB Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act (DNB Leidraad Wwft en Sw)

Version december 2020

DeNederlandscheBank

EUROSYSTEEM

Information for the reader

This concerns the section on sanctions regulations in the former DNB Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions (Leidraad Wwft en Sw, 2020), referred to below as the Guideline. In May 2024, the Guideline was replaced by DNB's Wwft Q&As and Good Practices.¹ The Wwft Q&As and Good Practices do not cover the Sanctions Act (Sanctiewet), given the impending legislative changes to this Act. We will in due course issue a separate policy statement regarding the Sanctions Act. The Sanctions Act section from the Guideline is provided below. There are no substantive changes to this section.

¹ <https://www.dnb.nl/en/sector-information/open-book-supervision/open-book-supervision-themes/supervision-of-financial-crime-prevention-integrity-supervision/>

1.1 General information

The Guidance issued by the Ministry of Finance provides extensive information on sanctions. In addition, a description is given below of DNB's supervision of compliance with the Sanctions Act 1997 (Sw) and the accompanying reporting procedure. The AFM and DNB have been entrusted with the supervision of compliance with the Sw with regard to financial transactions. To that end, the two supervisory authorities jointly adopted the Regulation on Supervision pursuant to the Sanctions Act 1977 (Regeling Toezicht Sanctiewet 1977). This Regulation states that an institution must take measures to verify whether customers of the institution appear on one or more sanctions lists (such as EU decisions and/or Regulations, decisions of the Dutch Minister of Foreign Affairs based on the Dutch regulation on terrorism sanctions 'Sanctieregeling Terrorisme 2007-II' – also referred to as the 'Dutch List'²– or UN Security Council Resolutions).

The European Union Regulations and national sanctions regulations describe several financial sanctions:

- orders to freeze financial assets of designated individuals and organisations
- a ban on making resources available to these individuals or organisations directly or indirectly
- a ban or restrictions on providing financial services (for persons, entities or goods)

An institution is expected to make its own risk assessment as a basis for measures to implement the sanctions regulations. This requires an appropriate risk analysis by the organisation, which can be developed within the SIRA system (see Chapter 3.2 – This reference is no longer current with the revision of the Guideline. DNB refers to *DNB's Wwft Q&A's and Good Practices*).

An institution must at all times be able to detect whether any of its customers are named in or its services and transactions relate to the sanctions regulations. An institution must also notify, or be able to notify, DNB of such cases without delay under Article 3 of the Regulation on Supervision under the Sanctions Act 1977. This requirement cannot be fulfilled on a risk basis, so the institution cannot opt to not comply with the sanctions regulations and dispense with the continuous screening of customers.

An effective screening process enables an institution to comply with sanctions regulations and is characterised by frequent screening. The screening times must be set in such a way that institutions are at all times in a position to find out whether their customers appear in or their services and transactions relate to the sanction regulations. The risk of violations of sanctions regulations can be reduced by screening at the time of acceptance, when relevant changes occur in the customer's position, when changes are made to the sanctions list and when transactions are effected.

² Zie voor de Nederlandse sanctielijst van personen en organisatie met bevroren tegoeden, <https://www.rijksoverheid.nl/documenten/rapporten/2015/08/27/nationale-terrorisielijst>.

Important screening times

- acceptance
- relevant changes in the customer's position
- changes in the sanctions lists transactions

1.2 Administrative organisation and internal control (AO/IC)

In its capacity as the supervisory authority, DNB assesses and enforces the effectiveness of the procedures and measures undertaken by institutions aimed at compliance with sanctions laws. In practical terms, when taking measures, an institution may seek alignment with existing administrative organisation and internal control (AO/IC) rules that arise from other regulations such as the Wft and the Wwft. The basic principle for the implementation of the AO/IC by the financial institution is that it should act in accordance with the objectives of the sanctions regulations. Briefly, this means that institutions are able to check their records in such a way that business relations, goods and transactions that are subject to sanctions can be identified. It must be possible to freeze the financial assets immediately and/or to prevent financial assets and/or services being made available.

No relationship with an existing customer must be terminated and in some cases dispensation may be sought from the Ministry of Finance. If the institution finds that the identity of a business relation matches that of an individual, legal person or entity referred to in the sanctions regulations (a so-called hit³), it must notify DNB immediately. The way in which hits must be reported to DNB is further explained in section 1.5.

In its assessment of the AO/IC, DNB looks, for example, at the following elements:

- The sanction risks that the institution incurs as recorded in the SIRA
- The design of the sanctions policy, the procedures and the codes of conduct
- The application of the institution's own sanctions policy in the customer files
- The screening process (including the handling and recording of hits)
- Training and awareness

³ An institution will encounter many potential hits when screening against the sanctions lists. These are all checked for correspondence with the various lists. Only genuine hits are reported. False positives are not reported.

1.3 The 'relationship' concept

The 'relationship' concept

The Regulations adopt a broad definition of the term 'relationship' covering any party that is involved in a financial service or financial transaction. This includes:

- customers
- representatives or authorised agents
- UBOs of the customers
- beneficiaries of a product (e.g. life insurance payments) or domestic or international transfers of funds
- counterparty to a financial transaction/ product (e.g. non-life insurance payments)
- person(s) involved in a financial transaction
- to which a company receiving services from a trust office is party
- directors of customers and parties related to customers

The term 'relationship' is defined so broadly because both the direct and indirect provision of financial resources or services falls under the sanction measures. In April 2013 new elements were added to the "Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy". These new elements state that the making available of funds to persons or entities that do not appear on the sanctions lists but are controlled or owned by persons or entities that do appear on the sanctions lists is in principle deemed to constitute the indirect

making available of funds to the sanctioned person or entity.⁴

Financial resources or services are made available indirectly if a person holds 50% or more of the ownership rights in a structure or if a person (for example a director) has control (which term is defined very broadly in the Guidelines). If the person holding 50% or more of the ownership rights or having control of an entity appears in a sanctions list, the assets of that entity must also be frozen and no funds must be released to it. In practice, institutions may also identify UBOs in the case of ownership percentages below 50%. It is therefore recommended that institutions apply the definition of UBO set out in the *Wwft* and therefore ascertain the identity of all UBOs holding 25% or more of the ownership rights, as institutions are prohibited from making assets available to persons or entities under the control of a sanctioned person. Control of an entity does not require ownership of 50% or more of the shares. There is a risk that UBOs will have control through various entities within a structure.

In the case of customers that are only partly listed on a stock exchange, it is important with regard to compliance with the sanctions regulations that the UBO of the unlisted part is known.

During the customer acceptance process, all relationships are defined and recorded in the relationship file. As well as the customer, this also includes other persons and entities involved in

⁴ Guidelines on implementation and evaluation of restrictive measures (sanctions). Available for consultation at: <https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/en/pdf>.

6

the financial service or transaction, such as the customer's UBO(s), representatives, directors, authorised agents and beneficiaries (where known). Since the term 'relationship' is defined so broadly, an institution surveying all relationships must assess the extent to which a particular relation has or can have ownership or control of the funds.

During the identification process, information is recorded such as the name, date of birth, place of residence and registered address of these persons and entities. This information enables the institution to perform proper checks. The absence of a date of birth or place of residence, for example, can make it more difficult to assess a hit. In the case of legal persons, it is generally sufficient to check the information contained in the Trade Register at the Chamber of Commerce, while for natural persons a check of a passport or a copy of the passport is generally sufficient to enable adequate screening against the sanction regulations.

In the case of relevant changes in the customer's position, for example a change in relationships or UBOs, an institution must update its customer database. In the case of relationships that qualify as high-risk (for example customers trading with sanctioned countries), an institution is expected to play a more active role in identifying changes. That can be done, for example, by conducting periodic enquiries to identify any changes in the relevant relationships. The full customer database can then be included in the screening process.

The institution must also investigate whether a ban or restriction applies to the financial service or transaction in relation to certain countries and regions and/or certain goods (embargoes). The institution must record this information in an accessible way.

Focus on strategic goods and proliferation

Some sanctions regimes include bans or restrictions on providing financial services for goods. These include, for example, military goods, 'dual-use' goods, strategic services (e.g. software and technology) and goods that can be used for internal repression (torture goods). [More information](#) on these goods (available in Dutch only).

1.4 Transaction monitoring

The principle is that the parties involved in transactions (relations) are screened against the sanctions lists. The institution must ensure that its AO/IC is configured in such a way that sanctions regulations are complied with even in the case of payments effected with the assistance of third parties. If sufficient agreements have been made with the third parties on compliance with the sanctions regulations, the institution can have confidence that the third parties will freeze assets if necessary. The agreements should include provisions whereby institutions inform each other of transactions that will be frozen and foreign third parties will also use Dutch sanctions lists during the screening process. The institution must ensure

that its AO/IC is configured in such a way that the objectives of the sanctions regulations are complied with even in the case of payments to third parties.

How does an institution filter transactions against sanctions lists?

Information or fields against which checks are carried out as a minimum:

- payer
- payee
- place names
- country
- description

Institutions conducting payments filter the SWIFT MT series and fields (including n99 messages) and SEPA messages and fields that the institution has identified on the basis of a documented risk assessment.

Trust offices, insurers and institutions with limited payment transactions carry out checks when making payments to beneficiaries as to whether the natural or legal person concerned appears on the sanctions lists

1.5 Reporting to DNB

7

In the event of a hit, the institution reports the following to the supervisory authority:

- ■ identifying data (name, alias, address, place and date of birth)
- ■ the nature and size of the frozen deposits or assets
- ■ the action taken by the institution
- ■ the applicable sanctions regulation(s)

Institutions send hits to DNB using the report format drawn up by the AFM and DNB.⁵ DNB assesses the completeness of the reports received from financial institutions. Institutions report the cases in which there is an actual hit. If an institution doubts whether a hit report represents a genuine hit, it must conduct further research to confirm or rule out a match with the sanctions lists.

Exemptions are possible in some cases (this may vary depending on the sanctions regulation). The Minister of Finance is authorised to decide on this. A substantiated request for exemption can be sent to the Ministry.

⁵ See also the DNB website: <https://www.dnb.nl/en/sector-information/supervision-laws-and-regulations/laws-and-eu-regulations/sanctions-act-1977/getting-around-in-sanctions-regulations>

Example of a grant of exemption

This concerns the special case of liability insurance. For example, a customer of an insurer who has taken out third-party liability insurance causes a collision. On settlement of the claim, the insurer has to pay damages to the victim/beneficiary. However, upon checking it transpires that the beneficiary appears on the sanctions lists, so the insurer is required to freeze the funds under the sanction regulations, whereas under other regulations it may have an obligation to pay out. In such cases, the institution freezes the funds and uses the report format to notify DNB, which then forwards the report to the Minister of Finance. On the basis of a substantiated exemption request, the Minister can then decide whether an exemption can be granted. In the case of other insurance policies where the beneficiary is unknown, the insurer must also check whether the sanction regulations apply when a claim is submitted.

7.6 Hit reports, FIU reports and deadlines

When institutions freeze assets on the basis of a hit on sanctions lists, they are also expected to look at the transaction history to see whether any transactions have taken place that could be assumed to be related to money laundering or terrorist financing. If money laundering or terrorist financing is suspected, institutions must report this to the FIU under Section 16 of the *Wwft*.

Assets must remain frozen until the relevant sanctions regulation is amended and the obligation to freeze the assets is lifted, an exemption is granted or notice to the contrary is received from the Minister of Finance or DNB. If the institution does not hear anything, it must assume that the assets are to be considered an actual hit and must remain frozen until further notice.

The reported data must be retained for a period of five years after the relevant sanctions regulation has ceased to have effect or has been rendered inoperative.

Supplementary information

Dutch government – International sanctions

<http://www.rijksoverheid.nl/onderwerpen/internationale-sancties>

Ministry of Foreign Affairs – Sanctions summary page – Restrictive EU measures

<https://ecer.minbuza.nl/ecer/dossiers/buitenlands-en-veiligheidsbeleid/sancties.html>

DNB – Sanctions Act 1977

[Sanctions Act 1977 \(dnb.nl\)](#)

DNB – Q&A on the Sanctions Act for non-life insurance companies

<https://www.dnb.nl/media/ua5dp5p1/q-a-sanctiewet-voor-schadeverzekeraars.pdf>

(available in Dutch only).

DNB - Sanctions screening for (incoming and outgoing) crypto transactions

[Sanctions screening for \(incoming and outgoing\) crypto transactions \(dnb.nl\)](#)

DNB – Guideline on the Sanctions Act for Pension Funds

<https://www.dnb.nl/media/q23b1w3t/naleving-sanctiewet-voor-pensioenfondsen.pdf>

(available in Dutch only).

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl