DeNederlandscheBank
EUROSYSTEEM

Q&A Feedback statement of September 16, 2022 on sanctions screening for (incoming and outgoing) crypto transactions.

DNB received seven responses. We welcome these responses, and have amended the Q&A in a number of areas. This feedback statement addresses the most important issues from the responses received in the consultation. Under "Amendment" we have indicated whether the response has resulted in any changes.

#	Subject	Details	Our response	Amendment
1	Need for further explanation regarding compliance with sanctions regulations[1]	The responses reveal that clarification is needed on the usefulness and necessity of this detailed explanation by DNB. There are various EU regulations that deal with the freezing of economic resources or funds of sanctioned entities, legal persons and natural persons. Failure to comply with such binding provisions is a criminal offence. This also applies to a crypto service provider that is deliberately or unwittingly involved in a transaction involving a sanctioned legal or natural person or entity. DNB is not charged with deciding whether to take enforcement action against institutions after they have been involved in a transaction involving a sanctioned legal or natural person or entity. We are charged with supervising the way in which institutions endeavour to prevent the processing of a transaction in which a sanctioned legal or natural person or entity	We have set out the obligations that institutions must meet to avoid facilitating a transaction involving a sanctioned legal or natural person or entity in the Regulation on Supervision pursuant to the Sanctions Act 1977. We limit ourselves to assessing the internal controls implemented to comply with the Sanctions Act 1977 (hereafter: the Sanctions Act) and the Regulation on the Supervision pursuant to the Sanctions Act 1977 (hereafter: *RtSw*) on the basis of a principle-based approach. If we find the measures taken to be inadequate, we will make use of the enforcement measures available to us (e.g. an instruction, a fine or an order subject to penalty). The Q&A is intended to provide further explanations to assist parties and clarify our expectations regarding compliance with relevant provisions.	No

[1] This document uses the term "sanctions regulations". This refers to the entire national and international body of sanctions regulations, including relevant EU regulations, the Sanctions Act (*Sanctiewet 1977 – Sw*) and the Regulation on Supervision pursuant to the Sanctions Act (*Regeling toezicht Sanctiewet 1977 – RtSw*).

		is directly or indirectly involved. In particular, we are charged with supervising the effectiveness of measures that institutions, including crypto service providers, must put in place to meet the requirements arising from the Sanctions Act 1977 and thus the requirements arising from the EU sanctions regulations governing the Act.		
2	We apply a broad interpretation to the term "relationship".	The responses we received on the draft Q&A give us reason to conclude that, in a number of concrete situations, there is a lack of clarity as to whether legal or natural persons or entities should be regarded as "relationships" of the crypto service provider. For example, there is uncertainty as to whether the holder of an external (hosted or unhosted) crypto address should be regarded as a relationship. Holders of an external (hosted or unhosted) crypto address who are involved in a transaction, either as payer or as payee of the transaction, are also considered to be a relationship of the crypto service provider. After all, the crypto service provider makes funds available to the holder of an external (hosted or unhosted) crypto address during an outgoing transaction. In an incoming transaction originating from an external (hosted or unhosted)	The objectives of European and other sanctions laws and regulations are broad: on the one hand, no funds or economic resources are to be made available, directly or indirectly, to legal or natural persons or entities listed in the sanctions laws and regulations and, on the other hand, all funds and economic resources belonging to, owned, held or controlled by legal or natural persons or entities listed in the sanctions laws and regulations are to be frozen. The Sanctions Act was drafted to implement European sanctions regulations, among other things. Pursuant to the Sanctions Act, we are responsible for ensuring that businesses implement their internal controls in such a way that they can comply with the aforementioned broad objectives of sanctions regulations. In order to perform this task, the term "relationship" was included in the *RtSw*. "Relationship" as used in the *RtSw* must therefore be interpreted on the basis of the broad objectives of sanctions legislation. A crypto service provider's relationships that are involved in an incoming and/or outgoing crypto transaction include at a minimum the crypto service provider's customers, the customers' ultimate beneficial owners, the counterparty to a	Yes

		crypto address, the crypto service provider must be able to establish whether the funds originate from a sanctioned party in order to determine whether the funds should be frozen and whether a hit should be reported to DNB.	crypto transaction and the payee or payees of a transaction. This is because these relationships dispose (at some point), directly or indirectly, of the funds that the crypto service provider makes available. The crypto service provider must assess whether additional parties are involved in the transaction to whom funds are made available either directly or indirectly. These parties are also considered to be relationships of the crypto service provider.	
3	Verification	Respondents note that the regulations do not provide an obligation to check or verify the identity of a relationship. Respondents also mention the disproportionate impact that a verification requirement may have on this sector and on smaller institutions in particular.	Providers of crypto services must at various points, including for every outgoing and incoming transaction, screen the relationships against the sanctions lists in order to be sure that no funds are made available to sanctioned legal or natural persons or entities, and to decide whether funds should be frozen because they originate from a sanctioned legal or natural person or entity. Relationship screening cannot be risk-based. Indeed, the moment a crypto service provider does not screen a relationship, there is no way for the crypto service provider to ascertain whether the relationship is subject to sanctions. If there is a risk that the specified identity is not correct, the provider will have to determine the actual identity of the legal or natural person or entity involved in the crypto transaction with certainty. Screening is not just about checking the name provided by the customer against the sanctions lists; the crypto service provider must take measures to establish whether the information provided is correct and therefore whether the crypto service provider may be involved in a transaction with a sanctioned legal or natural person or entity. The measures a crypto service provider takes to verify the identity may be risk-based. This	Yes

			means that it is up to the crypto service provider to assess the risk that it will execute a transaction involving a sanctioned legal or natural person or entity, and then to assess what measures are appropriate to mitigate the risk of non-compliance with sanctions regulations. In doing so, crypto service providers must take into account the high risk of non-compliance with, or evasion of, sanctions regulations that the provision of crypto services by its very nature entails. The crypto service provider must not accept the risk if no measures can be taken to mitigate the risk of a crypto transaction breaching sanctions regulations, if measures require too much effort or involve too much residual risk.[2]	
4	Are incoming and outgoing crypto transactions always high risk?	Several respondents requested clarification of the example of a high risk.	With regard to designating transactions to and from third parties as high risk, it should be noted that the term "third parties" can be interpreted in various ways: self-hosted (non-custodian) wallets, custodian wallets with service providers registered in the EU, custodian wallets with service providers registered outside the EU and custodian wallets with non-registered service providers. The risks may be different from case to case. Furthermore, as we noted earlier, all relevant factors must be included in the final (net) assessment of the risk. We will amend the text of the draft Q&A by pointing out the general – and high – risks of evasion of sanctions regulations when cryptos are involved, combined with the fact that crypto services are usually provided remotely. High risk is a blanket classification for various levels of risk that are seen as high. As an example, a crypto service provider may facilitate a transaction to a third-party wallet	Yes

[2] See also Financial Sanctions Regulation Guideline of the Ministry of Finance, p. 10.

			hosted by a provider registered elsewhere in the EU on behalf of its own customer who also holds a hosted wallet with the provider. In this case, the risk of failing to comply with sanctions regulations is not as high as in the case of a transaction facilitated to an unhosted wallet because a number of factual safeguards are in place that reduce the risk of non-compliance with sanctions regulations. These safeguards are lacking in a transaction with an unhosted wallet. The Q&A will be amended as follows: "Crypto services entail a high risk by their very nature, as the technology can facilitate a certain degree of anonymity of the crypto address holder and of transactions, and are almost exclusively provided remotely. This means that a greater degree of risk mitigation is expected from crypto service providers. There are different risks associated with each type of crypto transaction. For example, a crypto transaction involving a wallet hosted by another crypto service provider that has been registered under the same conditions differs in terms of risk from a crypto transaction involving an unhosted wallet. The risk of non-compliance with sanctions regulations is higher in transactions where the crypto address not hosted by a provider does not show to whom it belongs, as is the case for unhosted/private wallets. Crypto transactions from or to third parties therefore involve the risk of cryptos being transferred to, or received from, a person or entity referred to in the sanctions regulations. It is the responsibility of the crypto service provider to assess this risk and take adequate mitigating measures."	
5	Proportionality	A number of respondents indicate that the Q&A places a disproportionate burden	The size of a crypto service provider is not a decisive factor in determining the measures to be	No

		on the institutions. On the one hand, they point to the high regulatory burden in connection with the size of their organisation. On the other hand, they also say the nature of the controls that must be implemented is disproportionate.	taken in order to comply with sanctions regulations. Proportionality is the relationship between the controls and the nature and complexity of an institution's activities and the associated risks. Characteristics that may be indicative of the need for more intrusive measures are a high proportion of cross-border transactions and anonymity.	
6	Comparison with policy statements in other sectors	Respondents indicate that our standpoint on crypto service providers differs from existing policy statements for other sectors. For example, the current Q&A for non-life insurers on the same topic takes a different approach.	We understand the questions about other sectors, especially since some policy statements indicate that sanctions screening can be risk-based. We are of the opinion that sanctions screening cannot be risk-based (after all, the institution must continually know whether it is providing services to a sanctioned legal or natural person or entity, for example when executing transactions). In other words, institutions must i. establish the identity of their relationships, and ii. screen their relationships for hits against the relevant sanctions lists. It is up to the institutions to decide on how to do this and what these activities will require. Institutions can use a risk-oriented approach, provided it is properly substantiated and documented. However, relationships must always be screened. They can use a risk-based approach for the following, for example: a) The frequency of sanctions list screening for existing relationships. b) The verification of whether the relationship is actually the party for whose benefit a financial service or transaction is provided. If the risks of evading sanctions regulations are higher, then the process of establishing a relationship's identity and checking for hits must also be more intrusive. c) The technical aspects of the screening process. We will amend other policy statements to reflect this	No

			standpoint in the time to come, and in doing so we must ensure a level playing field for all parties. The Sanctions Act 1977 and *RtSW* are fully applicable to other sectors. Until then, we will clarify the status of relevant statements with the following addendum: "Some parts of this information are no longer current and will be amended. Please see the relevant news item." This will be included in the policy statements Q&A on the Sanctions Act for non-life insurers, the Guidelines on the *Wwft* and *Sw* (version December 2020) and Sanctions Check for Exchange Institutions.	
7a	Status of DNB's Q&As	Many respondents query the status of our Q&As and Good practices.	Please see our explanatory guide to policy statements: Explanatory guide to DNB's policy statements This Q&A provides insight into our supervisory practice and our interpretation of relevant open standards, specifically in regard to sanctions screening by crypto service providers. We publish Q&As and Good practices to provide the sector with more clarity on our expectations with regard to compliance with the Sanctions Act by the institutions under our supervision. Q&As do not offer self-contained supervision standards. Q&As are binding for DNB in the sense that an institution that acts in accordance with the Q&A can, in principle, rely on the fact that we consider their course of action to be appropriate. If institutions apply the relevant laws or regulations in line with a Q&A, we cannot deviate from it without good reason. An institution can therefore be assured that we will undertake our supervisory activities in line with a Q&A. Conversely, a Q&A is not binding for institutions. An institution may comply with the relevant laws or regulations in a way other than specified in the	No

			Q&A. In doing so, they must be able to demonstrate and substantiate that they comply with the legislation or regulations.	
7b	Questions about the status of DNB's Good practices	A number of respondents ask for clarification of the status of good practices. They also indicate that some Good practices could be revised for clarity.	The Good practices provide examples of measures that we have encountered in practice and that institutions can consider taking to control the risks of non-compliance with sanctions regulations. The document states: *Depending on the differences in risks, a more intrusive measure or a combination of measures may be chosen. The complete package of measures must be tailored to the specific risks of the customer and the transaction.* The response to the consultation reveals that some parties believe that the status of the Good practices and the objective that we hope to achieve by publishing them could be clarified. The current Q&A text provides a clear disclaimer regarding the status of the Good practices: *Good practices set out suggestions or recommendations for supervised institutions. These are examples of possible applications that, in DNB's opinion, provide a good interpretation of the obligations laid down in legislation and regulations. Good practices are indicative in nature and institutions are free to choose a different application as long as they otherwise comply with the law.* See the Explanatory guide to DNB's policy statements for further information on using the Good practices. Furthermore, specific parts of the Good practices will be amended: - "Very high-risk countries" will be changed to "countries subject to sanctions" - "External crypto addresses" will be changed to "crypto addresses not hosted by the provider"	Yes

			- "Blocking crypto addresses linked to illegal activities and addresses sanctioned by the US Office of Foreign Assets Control (OFAC)" will be changed to "Blocking crypto addresses linked to sanctioned entities and legal or natural persons" - "SIRA" will be changed into "integrity risk analysis that the provider must conduct in the context of *Wwft* compliance" - The subheading "Measures to establish whether the counterparty and/or beneficiary specified by the customer is in fact the recipient or the sender" will be deleted, and the lower bullets will be added to the list above it.	
9	Coherence with the General Data Protection Regulation (GDPR).	In their responses to the draft Q&A, we note that several parties point out the extensive processing of personal data involved in complying with the Sanctions Act and other sanctions regulations.	The GDPR applies to the processing of personal data by crypto service providers in their role as gatekeepers. The Dutch Data Protection Authority supervises compliance with the GDPR.	No