25 March 2024

**EBA Consultation on Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures (EBA/CP/2023/42)**

Dear Sir or Madam,

Although we welcome an EU-wide harmonization of sanction-related processes, due diligence obligations and controls, there are concerns with regards to some points of the present guidelines, which we would like to present to you below:

1. **Background and Rationale (Chapter 3.2, p. 7 ff, margin number 10)**

Guidelines:

“The first set of draft guidelines provides that financial institutions should:

1. (…)
2. (…)
3. carry out a restrictive measures exposure assessment, which should inform institutions’ decision on the types of controls and measures they need to apply to comply effectively with restrictive measures. **A restrictive measures exposure assessment cannot result in applying a risk-based approach towards the compliance with restrictive measures.** Restrictive measures policies, procedures and controls are commensurate to the restrictive measures exposure assessment to determine that all areas have the resources necessary to ensure compliance with the internal policies, procedures and controls for the implementation of restrictive measures.”

Remarks:

The meaning of the highlighted sentence is unclear and no clear content can be inferred from it. This is particularly because the result of a risk analysis ("restrictive measures exposure assessment") is intended to give the institution an overview of the risks to which it is exposed. On the other hand, this result subsequently represents the starting point for a risk-based approach when defining risk-mitigating measures. This is even explicitly stated in point c. above: "Restrictive measures policies, procedures and controls are commensurate to the restrictive measures exposure assessment (...)". However, the phrase "cannot result in applying a risk-based approach" contradicts this.

Proposal: The highlighted sentence is deleted without replacement.

1. **Draft Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures (p. 15 ff)**
	1. **Conducting a restrictive measures exposure assessment (margin number 24)**

Guidelines:

“Financial institutions should base this assessment on a sufficiently diverse range of information sources, including at least the following:

1. (…)
2. information from international bodies, government, national competent authorities including AML/CFT supervisors, FIUs and LEAs, such as up-to-date typologies on the circumvention of restrictive measures;
3. information from credible and reliable open sources, such as reports in reputable newspapers and other reputable media outlets;
4. information from credible and reliable commercial organisations, such as risk reports;
5. (…)”

Remarks:

In our view, points b. to d. are formulated too broadly, so that their scope and the actual sources to be used remain unclear.

* Do Austrian banks only have to take into account information from Austrian authorities and public institutions when preparing the assessment? Or are the relevant authorities of all EU member states to be used as sources of information?
* Which open source sources are to be classified as "credible" and "reliable" and which are not, and which criteria are to be used to assess credibility?
* Which media are to be classified as "reputable" and which criteria are to be used in the assessment?
* Is only information from the WKÖ as the responsible public commercial organization relevant for Austrian banks? Or are all public and private commercial organizations throughout the EU to be regarded as "credible and reliable commercial organizations"?
* Does the term "international bodies" only refer to EU bodies or also to international organizations worldwide?

Depending on the interpretation of the terms, this results in an enormous number of European or even global sources of information that banks must take into account when preparing the Restrictive Measures Exposure Assessment. Taking an excessive number of sources into account would involve an unmanageable amount of work. In our view, the sources to be considered should therefore be precisely defined and limited to a relevant level.

Proposal: Points b. to d. are replaced by the following point

"information from the EU Commission, the European Council, other EU bodies, the respective national government, the respective national competent authority (including the respective national competent AML/CFT supervisor), the respective national FIU and LEA, the respective national chamber of commerce, as well as publicly widespread media reports"

* 1. **Conducting a restrictive measures exposure assessment (margin number 26)**

Guidelines:

“Financial institutions should ensure that their restrictive measures exposure assessment remains up to date and relevant. To achieve this, financial institutions should review and, if necessary, update their restrictive measures exposure assessment in at least the following situations:

1. (…)

(…)

1. (…)”

Remarks:

The OeNB expects Austrian banks to prepare an annual sanctions risk analysis. The circumstances mentioned in points a. to e. are generally good indicators for the annual identification and analysis of sanction risks. The preparation of a complete, new risk analysis during the year or on an ad-hoc basis on each of these occasions represents a disproportionate effort with limited benefit. The scenarios mentioned in points a. to e. are analyzed and taken into account on an ongoing basis anyway when implementing and complying with sanction measures.

Proposal:

The highlighted sentence is replaced by the following wording:

"To achieve this, financial institutions should review and, if necessary, consider at least the following situations when updating their restrictive measures exposure assessment once a year."

1. **Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures under Regulation (EU) 2023/1113 (p. 33 ff)**
	1. **Screening the customer base (margin number 16)**

Guidelines:

“They should also list trigger events when screening should always take place and keep this list up to date. Trigger events should include at least:

1. (…)
2. for individual customers:
	1. (…)
	2. (…)
	3. **if reasonable grounds exist to suspect that the customer, or a person known to be connected with the customer, is attempting to circumvent restrictive measures.**”

Remarks:

What is meant by "person known to be connected with the customer"? Is this a shareholder, a member of management, an authorized signatory, an employee, a customer of the customer, etc.? This point is formulated too broadly to be able to derive a practical meaning from it. Moreover, this point has no relevance: if an alert is generated when screening the customer or a transaction in which the customer is involved, the customer is examined in detail and a decision is made in accordance with the dual control principle.

Proposal: The phrase "or a person known to be connected with the customer" should be deleted without replacement.

* 1. **Screening the customer base (margin number 17)**

Guidelines:

“PSPs and CASPs should screen at least the following customer information, in line with the applicable restrictive measures:

1. for natural persons:
	1. the first name and surname, **in the original and transliteration of such data**; and
	2. **date of birth**
2. for legal persons: the legal name, **in the original and/or transliteration of such data**;
3. for both natural persons and legal persons: any other names, aliases, **transcriptions in other alphabets**, trade names, where available in the restrictive measures-related lists.”

Remarks:

Ad „original“, „transliteration“ and „transcriptions in other alphabets”:

If the customer's name is not written in Latin letters, only the Latin transcription is recorded in the core banking system anyway; the original (e.g. Cyrillic) spelling is not recorded. Different spellings in the Latin transcription are covered in the screening by fuzzy logic.

"original" and "transcriptions in other alphabets" can only be understood to mean that in addition to the customer-name in the Latin spelling, spellings in other alphabets should also be recorded and screened. Consequently, this means, for example, that the name of a Russian customer should be recorded both in the Latin transcription and in its original/Cyrillic spelling, as well as in other (!) alphabets (Arabic, Chinese, Korean, Japanese).

Every bank would therefore have to have appropriately linguistically competent staff who speak Russian, Arabic, Chinese, Korean, Japanese, etc. and understand the corresponding alphabet language and the corresponding alphabet. A corresponding adaptation of the core banking system and an expansion of the screening software would also be necessary.

This requirement, including the consequences outlined above, is neither necessary nor proportionate (given the considerable additional effort and costs). As already explained above, recording the customer name in its Latin transcription is sufficient. The recording of different transcription variants is ensured by fuzzy logic.

Ad „date of birth“:

If the screening of the name triggers an alert, this can be (manually) checked for plausibility using the date of birth as part of alert processing. This method is a common procedure. In our view, it should therefore be left to the PSPs/CASPs to decide whether to take the date of birth into account during the screening process or to manually check it during age handling.

Proposal: The phrases "in the original and transliteration of such data", "date of birth", "in the original and/or transliteration of such data" and "transcriptions in other alphabets" should be deleted.

* 1. **Screening the customer base (margin number 18)**

Guidelines:

“When screening customers that are legal persons or natural persons, PSPs and CASPs should, to the extent that this information is **available**, also screen:

1. **beneficial owners**;
2. **persons authorised to act on behalf of the customer**;
3. **persons connected to the customer, such as natural and legal persons within the management or ownership structure**, who may be controlling/exercising a dominant influence on the entity as defined in Article 1 of Council Regulation (EC) No 2580/2001.”

Remarks:

Ad „available“:

All relevant information on the customer has already been collected as part of the KYC required under money laundering law and regulated in detail. This information must also be used for the purposes of sanctions compliance in order to establish parallelism between AML and sanctions KYC. Therefore, "available" should be clarified to this effect.

Ad "beneficial owners": The Guidelines should clarify that "beneficial owners" are to be understood as "beneficial owners" within the meaning of Art. 3 no. 6 of the 4th Anti-Money Laundering Directive. This ensures that information obtained in the context of KYC under money laundering law is also sufficient for sanctioning purposes. The term "beneficial owner" is based, among other things, on a shareholding of more than 25%. From a sanctions law perspective, such a level of ownership is more than sufficient, especially as the concept of ownership in EU sanctions law is based on a higher ownership threshold (more than 50%).

Ad „persons authorised to act on behalf of the customer“:

This point is formulated very broadly and unclearly. Does it refer to members of the board or management? Or authorized signatories? All employees of the company who represent the company externally (sales, purchasing, legal department, external third parties with power of attorney)? In order to achieve consistency with AML regulations, this point should sensibly be restricted only to persons who act as authorized signatories vis-à-vis the bank and thus have access to the company's credit balances/securities.

Ad "persons within the management": Only members of the board of directors or management who are authorized signatories can dispose of the funds and securities held at the bank. Screening all members has no added value as long as all members do not have to be recorded anyway for AML reasons (e.g. to determine subsidiary owners).

Ad „persons within the ownership structure“:

This wording is very imprecise and, in our view, requires clarification. It is not clear whether only the direct owners or shareholders are meant or whether other levels of ownership are to be included. Recording all levels of ownership would represent a disproportionate additional expense without any recognizable added value, unless this is already required for reasons of money laundering law. The recording of direct and indirect owners in accordance with money laundering regulations is sufficient for sanction purposes due to the AML-relevant threshold of 25%, as the relevant threshold for sanctions only starts at 50% plus 1 anyway.

Proposal:

Ad „available“: The term is to be replaced by "available as consequence of the application of the financial institution’s customer due diligence measures, in compliance with the provisions of Article 13 of Directive (EU) 2015/849".

Ad „beneficial owners“: The term is to be replaced by „beneficial owners as defined by Article 3 (6) of Directive (EU) 2015/849 as amended”.

Ad „persons authorised to act on behalf of the customer”: The wording is to be replaced by „authorised signatories to the PSP or CASP“.

Ad point c.: If consistency with AML requirements cannot be achieved in this point (in particular through the above-mentioned proposal to specify the term "available" in the sense of already existing KYC information in accordance with the 4th AMLD), we propose the following alternative: Only in the case of certain risk indicators in the ownership chain that have been previously defined (e.g. sanctioned minority owners identified in the KYC process) should a risk-based determination of the owners also take place in the second or further levels.

* 1. **Policies and procedures for the management and analysis of alerts (margin number 32)**

Guidelines:

“Such policies and procedures should include:

1. (…)

(…)

1. different levels of review to be carried out, for example the discard of false positives approved by at least two people.”

Remarks:

Alert handling staff undergo detailed training before starting their work. They keep their knowledge up to date through regular (also ad-hoc) training and a regular information exchange with other colleagues about current cases and frequently encountered case constellations. For the reasons mentioned, obvious and easily recognizable false positive alerts can be rejected by a single person. The reasons for rejecting an alert are also documented in writing and can therefore be checked at any time. Processing by two people represents an unacceptable amount of additional work.

Proposal: The phrase "discard of false positives" in point d. is replaced by

"discard of complex false positives".

* 1. **Assessing whether an entity is owned or controlled by a designated person (margin number 37)**

Guidelines:

“PSPs and CASPs should:

1. (…)
2. (…)
3. use available public sources of information, such as lists of owned and controlled entities and beneficial ownership registers.”

Remarks:

The beneficial owners are already determined and regularly updated as part of the KYC required under money laundering law. Repeatedly consulting the relevant registers therefore has no added value.

Proposal: The words "and beneficial ownership registers" are deleted without replacement.

* 1. **Controls and due diligence measures to comply with sectoral restrictive measures (margin number 42)**

Guidelines:

“Examples of controls PSPs and CASPs may also put in place include, but are not limited to:

1. (…)

(…)

1. using the following data: shipping registers, real estate records and other publicly available data sets (**where available**).”

Remarks: "Where available" can potentially be interpreted very broadly. Searching public registers (some of which are subject to a fee) from all countries in the world represents an unreasonable or disproportionate effort.

Proposal: The phrase "where available" is replaced by "where available as consequence of the application of the financial institution's customer due diligence measures, in compliance with the provisions of Article 13 of Directive (EU) 2015/849, or where such information can be obtained with reasonable effort".

* 1. **Reporting measures (margin number 50)**

Guidelines:

“When suspecting a possible circumvention of restrictive measures, or detecting an attempted transfer of funds or crypto-assets to a designated person, entity or body, PSPs and CASPs should:

1. **report it to the national authority competent for the implementation of restrictive measures**;
2. if the circumvention of restrictive measures is a crime that constitutes a predicate offence to money laundering in the Member State where the PSPs and CASPs operate, promptly submit a suspicious transactions report (STR) to the domestic FIU where the requirements set out under Article 33(1)(a) of Directive (EU) 2015/849 are met.”

Remarks:

EU sanctions regulations do not provide for a reporting obligation of this general nature. If an act of circumvention leads to a freeze of funds (e.g. because the identity of the true beneficial owner has been concealed), these will be reported to the NCA anyway. However, it cannot be ruled out that PSPs and CASPs will be obliged by national legislation to report such circumvention (apart from the asset freeze).

Reporting circumvention attempts to the NCA without an explicit (EU) legal obligation is fraught with legal uncertainty with regard to data protection and banking secrecy and could potentially lead to legal consequences (e.g. penalties for breach of data protection or banking secrecy). In addition, reporting to the NCA and the FIU at the same time involves duplication of effort, which can be avoided through increased data exchange and better coordination between the NCA and FIU.

Proposal: Point a. is deleted