ING Bank Slaski S.A. KYC Risk Appetite Statement

(Correspondent Banking RAS Poland)

Ver 2.1 – External
December 2023

Introduction

Correspondent banking relationships encompass a higher Financial and Economic Crime ("FEC") risk, in particular cross-border correspondent banking relationships involving the execution of third-party payments and trade finance. ING Bank Śląski S.A. hereinafter referred to as the Bank defines a correspondent banking relationship when:

- The Bank has an enabled SWIFT Relationship Management Authorisation ("RMA") Key either to send and/or receive authenticated traffic;

and,

banking services by one bank as the correspondent to another bank as the respondent are provided, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, foreign exchange services and trade finance services.

Correspondent banking does not include one-off transactions or the mere exchange of RMA keys in the context of non-customer relationships, but rather is characterized by its on-going, repetitive nature. This Correspondent Banking Risk Appetite Statement outlines the principles and standards for the Bank's approach to correspondent banking FEC risk management, to ensure uniform application throughout the bank. All employees and contractors of the Bank working with bank relationships are subject to this statement. This statement is published to the Bank's external stakeholders such as respondent banks, regulators and investors to inform them of our correspondent banking FEC risk appetite.

Expectation:

In accordance with the account terms[1], the client shall;

- have implemented appropriate measures with respect to Payment Orders sent to ING in order to comply with any anti-money laundering, anti-terrorism and sanction laws and regulations applicable to it;

- verify that none of its Customers is the subject of sanctions under any economic sanction laws (including, but not limited to, sanctions mandated by the United Nations or the Office of Foreign Assets Control of the U.S. Department of the Treasury and having effect under the laws of the jurisdiction of the Customers' incorporation or of the place of their habitual residence, as the case may be) that are relevant in connection with the Payment Services and that apply to the Client in respect of its Customers or any of them;

- not use a Payment Service for activities or purposes that are in violation of any law or regulation, or that can have a detrimental effect on the reputation of ING or on the integrity of the financial system.

If there are reasonable grounds to suspect a security breach then the Client must inform the Bank immediately and co-operate with the Bank and provide the Bank upon request with any information and documents and performs all such acts which the Bank requires (a) by law, regulation or according to the Bank's internal policies and procedures for the provision of the Payment Services and the execution of Payment Transactions, (b) to comply with requests of local and foreign (tax) authorities, and (c) for purposes of combating money laundering practices and terrorism financing, fraud and maintaining transparent and sound financial markets.

Regulatory Guidelines

The Bank is supervised by the National Bank of Poland and the Polish Financial Supervision Authority as part of supervisory mechanisms. The NBP and the PFSA are state regulatory bodies that monitor compliance with the relevant provisions on sanctions and protection against economic crime.

As with all ING entities, the Bank must ensure the full implementation of applicable local, EU and extraterritorial laws and regulations as well as the FC RAS Poland assumptions which are consistent with INF Group Global RAS requirements. Violation of applicable local, EU and extraterritorial laws and regulations may result in significant legal or reputational risk for the Bank and / or personal liability of employees.

[1] For a detailed overview of all account terms, please revert to the Byelaw for opening and maintaining LORO Accounts and for the execution of LORO Clients' Payment Orders.

High Risk Counterparties & Industries

Respondents that have significant levels of their business in high risk industries potentially pose an increased risk for ING. ING will carry out pre-transaction screening and post-transaction monitoring processes. Transactions received from a respondent that are not within the acceptable limits stated in ING's policy will be rejected. The respondent will be reminded of the Bank's policy and may be asked to refrain from sending such transactions. Please find below a list of high risk counterparties & high risk industries.

- Shell Companies: the Bank will not maintain relationships with banks whose client base is determined to be only or predominantly comprised of Shell Companies by means of transaction value or volume. The Bank will not process transactions of respondents that are made for or on behalf of known Shell Companies;
- "Non-domestic counterparties" without economic presence: Clients determined to have a disproportionate[2] number of non-resident accounts in their books. That is, clients not residing in or conducting business from the country where they have opened an account.
- Downstreaming: Downstreaming can expose ING to the risk of clearing transactions that are outside of the Bank's risk appetite, due to the reliance on the respondent bank's and/or downstream respondent bank's FEC Policy Framework. Bearing in mind these inherent risks, the Bank has limited appetite to downstream payments for its respondent banking relationships, in which case, additional assessment on the respondent bank as well as the downstream respondent bank could be required. Please note that double downstreaming[3] is never allowed;
- Politically Exposed Persons (PEPs);
- Commercial real estate activities;
- Armament manufacturers, dealers and intermediaries;
- Cash (and cash equivalent) intensive businesses;
- Money service businesses;
- Casino, betting and other related gambling activities[4];
- Pornographic activities[4];
- Non-profit organisations (especially those operating on a cross-border basis and those that are not regulated, registered or certified);
- Dealers in high value goods (e.g. art and antique dealers and auction houses), or precious metals and stones;
- Oil and gas (including exploration, oilfield services and gas sales);
- Cannabis industry[4];
- Virtual asset service providers, to the extent they are regulated and permitted by the
- relevant regulatory authority to provide such services on the financial markets in the EU, OECD or Singapore;
- Embassies and consulates;
- 'Gatekeepers' such as accountants, lawyers, or other professional service providers.

If a respondent does not respond to requests to refrain, the Bank may terminate the account agreement

Prohibitions

The Bank is prohibited from entering into or maintaining customer and business relationships involving:

- Anonymous accounts, anonymous passbooks and anonymous safe-deposit boxes;
- Accounts for shell banks and for financial institutions known to allow their accounts to be used by a shell bank;
- Accounts for unregulated/unlicensed financial institutions and for financial institutions known to provide banking services to unregulated/unlicensed banks;
- Correspondent relationships from non-recognised countries;
- Accounts for Money Service Businesses (MSBs) & Payment Service Providers, not maintaining a license (or exemption thereof) by an ING recognized regulator.

[2] Disproportionate is defined as >10% of the portfolio or revenue of the bank

[3] Double downstreaming: when a downstream respondent bank is offering ING's correspondent banking services to their respondent bank.

[4] Within specific limits and requirements, otherwise prohibited

- Virtual Asset Service Providers[5]
- Where there is, or is perceived to be, a risk of a UHRC nexus, unless the conditions related to UHRC nexus have been met;
- Bearer shares companies, unless the conditions related to bearer shares have been met;
- Persons and entities that are subject to sanctions which oblige the Bank to freeze their assets, unless the conditions related to handling of true hits have been met (including the initiation of the freeze procedure as applicable);
- Payment Service Providers with customer groups/sectors outside the Bank's risk appetite (i.e., customer groups/sectors to which the Bank would not be offering banking services directly);
- Payments Services Providers with entities offering downstream services to customer group/sectors deemed outside the Bank's risk appetite.
- Payable Through Accounts are not permitted: accounts maintained at the Bank as part of correspondent banking relation cannot be made directly available to the respondent's clients or third parties.

The list of high risk counterparties/industries and prohibitions mentioned in this concise risk appetite statement are not exhaustive. For questions or clarifications, please contact your relationship manager.

End of document

[5] As per FATF Recommendations (Financial Action Task Force is the global money laundering and terrorist financing watchdog. It sets international standards that aim to prevent these illegal activities and the harm they cause to society.): 1) "Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset". 2) "A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations."