



AML QUESTIONNAIRE

1. General information

Name of the business entity		PRIVREDNA BANKA ZAGREB D.D.	
Address of the registered office		Radnicka cesta 50, 10000 Zagreb, Croatia	
Legal form		Join stock company	
Trade and Companies Register		Commercial court, Zagreb	
Trade and Companies Register Number		080002817	
Public Company/Private Company		Private	
Legal Entity Identifier (LEI)		549300ZHFZ4CSK7VS460	
Shares publicly Quoted		No	
Fatca status		Compliant	
Global Intermediary Identification Number(GIIN)		D911IN.00059.ME.191	
Date of Establishment/Incorporation		7.4.1966.	
VAT No.	Telephone No.	SWIFT address	AML Department e-mail address
02535697732	-	PBZGHR2X	sprjecavanje.pranja.novca@pbz.hr
Official website		www.pbz.hr	
Total number of employees		3301	
If applicable, please provide details on Parent Bank	Name	Intesa Sanpaolo S.p.A.	
	Country	Italy	
If applicable, please provide details on Subsidiaries *in case more than five please fill in on separate sheet	Name	Intesa Sanpaolo banka d.d.	
	Country	Bosnia and Herzegovina	
	Name	Intesa Sanpaolo banka d.d.	
	Country	Slovenia	
	Name	PBZ CARD d.o.o.	
	Country	Croatia	
	Name	PBZ LEASING d.o.o.	
	Country	Croatia	
Name of primary Regulator/Supervisory Authority		CROATIAN NATIONAL BANK (CNB)	



2. Beneficial Owner and Senior Management

Information about the Ownership	The shares of PRIVREDNA BANKA ZAGREB d.d. are 100% held by Intesa Sanpaolo Holding International S.A., whose shares are 100% held by Intesa Sanpaolo S.p.A. (publicly traded on Euronext Milan – the Italian stock exchange). Based on the available information and to the best of our knowledge, there is no legal entity or natural person, including family members, that collectively own directly and/or indirectly 10% or more of the entity's shares. https://group.intesasanpaolo.com/en/about-us/shareholder-base/sanpaolo-imi Please find the document "Ownership Structure Statement" on the link https://www.pbz.hr/document/documents/PBZ/ostalo/KORPORATIVNI-DOKUMENTI/PBZ-Ownership-Structure-Statement-2026.pdf
Beneficial Owner	Further to the above statement, we consider all our Management board members as a subsidiary owners of the Bank. Please find all information on the official Bank's website or using publically available sources (The Business register of Republic of Croatia, typing in the field "OIB" VAT number of the Bank https://sudreg.pravosudje.hr/ords/r/esudreg/public/pretraga-subjekata#rez_1)
Management Board (PEP role)	Please note that no politically exposed person holds the position of Managent Board member.

3. Business activites information

Please fill in your business structure as a percentage of total business (e.g. Retail Banking, Corporate, etc.)

Business type	%	And of which (in %)	
		Residential	Non-residential
Retail	94	94	6
Corporate	6	99	1
Other			



Are You dealing with below listed customers or industries? If yes, please note what AML/CTF measures do you apply?

	Non-account holders	Offshore customers	Shell banks	MSB/MVTS customers	Arms, defense, military	Precious metals and stones
YES	✓	✓		✓	✓	✓
NO			✓			
State AML measures your institution apply	Please note walk-in customers cannot conduct crossborder payments, only domestic payments. Those in the amount equal or grater than 1.000 EUR undergo identification and verification, while those greater than 10.000 EUR undergo KYC procedure. Most of these type of customers come for paying utilities costs.	EDD	Prohibited	EDD	EDD The Bank is applying restrictive approach in regard to transactions involving controversial and/or banned arms, and the financing activities are allowed only if attended for armament materials intended for definitive use by armed forces and their defence bodies as well as police forces of countries belonging to the European Union and/or NATO or if it is present intergovernmental program with EU country or if the financing is within the framework of the "ReArm Europe Plan/Readiness 2030.	EDD
	Virtual currencies	Marijuana	Gambling	Unregulated charities	Regulated charities	Non-government Organization
YES			✓		✓	✓
NO	✓	✓		✓		
State AML measures your institution apply		Prohibited	Restricted while Internet gambling is prohibited	Prohibited	EDD	EDD



Does your institution conduct business in any of the restricted or sanctioned Countries (Iran, North Korea, Syria, Sudan, Cuba, Crimea)?	No
Does your institution provide Nested accounts or Downstream Correspondent Clearing Services?	No
Does your institution provide PTAs (payable through accounts) ?	No
Are you registered for or engaged in Money Value Transfer Service (MVTs)/ Money Service Business (MSB)	No
Are you engaged in the production and/or purchase/sale of weapons?	No
Are you registered for or engaged in cryptocurrency trading?	No

4. AML Policies and Procedures

Is your bank obligated by the local law to comply with applicable AML/CTF legislation?	Yes
Please provide applicable legislations	The Bank is required to comply with the Croatian Anti-Money Laundering and Terrorist Financing Act and applicable EU AML/CFT legislation. This includes the EU AML Package (Directive (EU) 2015/849, Regulation (EU) 2015/849 and Regulation (EU) 2015/849), as applicable, as well as other relevant EU AML/CFT legislation, including Directive (EU) 2015/849, Regulation (EU) 2015/849, Commission Delegated Regulation (EU) 2016/1675 and Commission Delegated Regulation (EU) 2019/758. The Bank is monitoring and implementing the requirements arising from the EU AML Package in accordance with the applicable entry-into-force and application timelines established by the relevant EU legislation.
Has your institution established written policies, procedures and controls in accordance with FATF International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation (The FATF Recommendations)?	Yes
Does your institution have AML policies and procedures in place ?	Yes
How often does your bank review AML policies and procedures?	Yearly
Are AML policies and procedures approved by Management Board?	Yes
How often do you provide AML training to your employees?	At least once a year



In what way is AML training provided to your employees?	Via active classroom and online
Do you have a procedure in place to check whether employees have at least basic or minimum required knowledge of AML processes and procedures?	Yes
Are all your employees obligated to attend AML training?	Yes
Are AML policies and procedures available to all your employees, and at all times?	Yes

Please provide information on who do you consider as PEP and how do you determine PEP as well as what AML/CFT measures do you apply?	PEP is any natural person who acts or has acted during the at least previous 12 months at a prominent public function in a member state or a third country, including their immediate family members or persons known to be close associates of a politically exposed person. PEP clients are assigned with a high risk level and therefore undergo EDD measures. Onboarding or continuation of a business relationship with a PEP client must be approved by the AML officer and Senior management.
--	--

Do you screen customers including their UBO against: (please select all that apply)		Upon onboarding	KYC renewal	Trigger event	Automated	Manual
	Sanctions	✓	✓	✓	✓	✓
	Penalties	✓	✓	✓	✓	✓
	Negative news	✓	✓	✓	✓	✓
	PEP	✓	✓	✓	✓	✓

Do you screen transactions against Sanctioned lists?	Yes			
Select the lists that your institution screens through the customer base?	US(OFAC)	UN	EU	name OTHER that applies
	✓	✓	✓	UK and internally developed lists
Does your institution have customers which are subject to UN, EU, US (OFAC) or other sanctions or applicable blacklists; or bank customers, branches, or subsidiaries that operate in countries subject to UN, EU, US (OFAC) or other sanctions or applicable blacklists?	No			



Does your institution maintain direct business relationships with customers (individuals or companies) located, domiciled or registered in high risk third countries?	The Bank may establish a business relationship with person from high risk third countries, provided that enhanced due diligence confirms that all internally prescribed conditions have been met, such as the person having valid residence in the Republic of Croatia, the purpose of opening the account being logical and documented, and the signing of the appropriate declarations (for persons from certain high risk third countries – for example customers from Iran and Syria declare they should not conduct transactions in USD).
Does your institution have in place a procedure to monitor transactions?	Yes
What is the method used to monitor transactions for suspicious activities?	Combination of automated and manual. We have an automated transaction monitoring technology in place (implemented software) through which all transactions are constantly monitored. Additionally, we also have procedures in place to conduct manual reviews after receiving informations from our branches which are then individually handled.
Which vendor and which procedures you apply in the process of monitoring transactions?	We monitor all cross border and international transactions (SWIFT and SEPA) and certain domestic payments on a risk based approach and in the real time through Norkom/Detica and through NetReveal by solving TxM alerts generated by various scenarios. Mentioned transactions are monitored in real time performing four-eye principle. The bank will not carry out a transaction for which it cannot determine the logic and purpose and may request documentation that supports the purpose prior to the execution of the transaction. Furthermore, we have TxM alerts in case any suspicious activity which needs to be resolved individually. In addition to this automated process, we have manual process in place which involves teller workers to submit an information about any suspicious behavior or activity of the client. We provide yearly education on this matter and encourage teller workers to submit report of any suspicious activity. We also use NetReveal for name screening against WCH lists including sanctioned countries, entities, and individuals.



Describe procedure in case transaction originates or involves a Sanctioned Entity or Country?	In case a client becomes subject to the sanctions, we report the client to the relevant bodies, block the account and initiate termination of the business relationship. Transaction will be rejected and as such reported to the local FIU.
Is any part of sanctions programme outsourced to the third party entity?	Yes. Only certain sanctions screening activities are subcontracted to be performed on the first and second level by third parties (name screening, payment filtering). Exelia-Intesa Sanpaolo Romania, as a part of the same bank group (ISP) is a centralized function for name screening and payment filtering activities. There is also a third level of control if there is a possible true match and it is conducted by the PBZ AML Department for final closing of the alert or transaction/payment release. Additionally, Quality Assurance is periodically performed as a control of these activities.
What is your procedure in case you receive incomplete SWIFT message?	The SWIFT Message will be automatically stopped in Bank's payment system before execution of transaction and it will be required from the sender bank to supplement the payment order with all necessary information and if not done the SWIFT message will be return to the sender.
Please indicate the authority to which you report suspicious transactional activities and person in respect of money laundering/terrorism financing	MINISTRY OF FINANCE, Office for the Prevention of Money Laundering and Terrorist Financing.

Do you apply risk based approach to all your customers?	Yes
What risk levels have you determined?	Low, Medium Low, Medium High, High, Unwanted
When does your customer gain risk level?	The Bank is obliged to identify and verify the identity of all clients with entering in the Bank's applications and by obtaining KYC Questionnaire therefore the client gains risk level immediately, before establishing a business relationship (in real time) or conducting the transaction. Further calculation is based on fingerprint mechanism or by ad hoc change.
Please describe EDD measures you apply?	Measures of enhanced due diligence are in addition to: determining the identity of the client,



	the ownership structure, beneficial owner, source of funds and the nature and scope of the business relationship/activities. This also includes collection of additional documentation related to the purpose of the business relationship (full scope of all non-residents and LE owned by non-residents). EDD includes the verification of the business relationship by the Competence Center and the AML department, and in some cases by Senior management. Bank has created several specialized forms for PEPs, Iranian, Russian/Belorussian entities, non-profit organizations, which are focused of assessment of risk that this type of clients presents and are verified by Competence Centers and AML Department (and Senior Management for PEPs) . The Bank also applies enhanced due diligence measures in the credit process.
For which customers do EDD measures apply?	For clients and transactions assessed as medium-low, medium-high, or high risk, the Bank implements enhanced due diligence measures, which may include applying some of the following controls depending on the specific situation: mandatory monitoring of all areas of the client's business and business relationships closer monitoring of their transactions an increased level of ongoing monitoring and review of the business relationship In accordance with ISP Group policies, the Bank collects information regarding the source of funds and the source and value of wealth (including income and assets), at a minimum for clients assessed as medium-high or high risk.
How often is periodic review applied?	For high risk clients every 12 months, while for medium high risk clients every 24 months, medium low every 48 months and low risk clients every 60 months.
What are the contributors upon which risk level is determined?	To calculate a client's risk, the Bank has defined 8 risk groups comprising multiple individual risk factors with varying risk weightings; in addition to these groups, it also employs certain special risk categories. Consequently, all factors are mapped to specific groups, with each factor belonging to only one group. Those groups are : Channel risk, customer risk, Geography risk, Industry risk, Occupation risk, Operations risk, Product risk and Relationship Duration risk. In addition to these, Related Parties risk (UBO risk) can affect a final risk of client.
Is risk level generated manually, automatically or both?	Automatically



Does your institution determine source of funds? Please provide details on the processes	Yes, through KYC Questionnaire we request for information on source of funds and also request documentation confirming the source. This also can be determined through ODD or EDD procedure. Furthermore, we collect this information while performing transaction equal or grater than 10.000,00 EUR and regardless the amount in case any suspicions.
Do you always aim to determine UBO of your customer?	Yes
If yes, what percentage do you take as relevant?	25%. Please note that even lesser ownership percentage (10%) can be applied if UBO can be identified.

Has your entity received any administrative penalties from any regulator, due to AML/CTF omissions or oversights in <u>last 3 years</u> ? If yes, please provide details and dates.	No
--	----

When was last audit performed	Name	Date	Were there any AML deficiencies found
From regulator	Croatian National Bank (HNB)	June 2023	No
External Audit	Ernst&Young	March 2026	No
Internal Audit	Privredna banka Zagreb d.d.	December 2025	No

5. Information about AML team

How many full-time AML employees do you have?	28
To whom does your AML team report to (in your institution)?	Management Board

Zagreb, 8.10.2026.

Please note In the event of any changes, this document shall be updated accordingly.