Risk Appetite Statement of MagNet Bank in connection with the Prevention and Combating of Money Laundering, Terrorist Financing and Proliferation Financing, and the Implementation of Financial and Asset-Related Restrictive Measures

General Principles

The Bank defines its risk appetite as the level and type of risk it is willing to accept in pursuit of its business objectives while maintaining compliance with applicable legal and regulatory requirements.

It is the firm objective of MagNet Magyar Közösségi Bank Zrt. (MagNet Hungarian Community Bank Plc.) to implement the prohibitions and procedures set out in Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter: AML Act) and its implementing decrees, as well as Act LII of 2017 on the Implementation of Financial and Asset-Related Restrictive Measures Ordered by the European Union and the United Nations Security Council (hereinafter: Sanctions Act), while taking into account relevant international and domestic recommendations and best practices, so that its operations reflect not only the letter but also the spirit of the law.

To this end, MagNet Hungarian Community Bank Plc. and the entity(ies) subject to consolidated supervision together with it (hereinafter collectively referred to as the "Bank") carry out their activities related to the prevention and combating of money laundering, terrorist financing and proliferation financing in accordance with the principles set out below. In order to protect our Bank and, more importantly, our customers, our business policy is to implement the highest and most effective standards of combating financial crime, which might result in the Bank not being able to support certain business activities even if those comply with local AML and CTF requirements, or with such requirements applied by other financial market participants.

The Bank maintains a zero tolerance approach to all criminal activity, we are committed to fighting all forms of financial crime and we will do our utmost to ensure that the products and services we offer are not used for money laundering, proliferation or terrorist financing or fraud.

The Bank does not provide any products or services to any natural or legal person who is subject to sanctions.

Our Bank reserves the right to refuse any customer relationship, transaction or business instruction if it is not in accordance with its Risk Appetite.

The Bank operates mandatory internal procedures that are binding for all its employees, its internal regulations fully comply with FATF recommendations, Directive 2015/849 of the European Parliament and of the Commission and Council of Europe Regulation 2015/847. The declarations required by international regulations are available on the Bank's website.

Establishment of a Business Relationship

The Bank applies customer due diligence (CDD) and enhanced due diligence (EDD) in accordance with the relevant legislation.

The Bank will not establish customer relationships, or will terminate existing relationships with customers where there is reason to believe that the customer:

- refuses to provide sufficient information or documents that would allow them to be fully identified or with which they can support their compliance with the standards of this Statement;
- intentionally violates or acts with willful negligence towards laws, rules and procedures related to the prevention of financial crimes;
- regularly violates, intentionally or recklessly, laws, rules and procedures for the prevention of financial crimes
- uses a bank account for money laundering, proliferation or terrorist financing, fraud, or conducts business activities that may constitute a tax crime.

The Bank does not establish business relationships with businesses or persons whose activities involve a high risk or whose chosen operating structure falls outside the Bank’s risk appetite. In particular, it does not enter into any relationship with

- Companies involved in the organisation of gambling (except for state-licensed operators),
- Businesses involved in arms trading, except for enterprises duly authorised by the competent authority and operating as contracted partners of the Ministry of Defence in close cooperation with it,
- Businesses and individuals involved in illegal narcotics trafficking, pornography, human trafficking, and other serious criminal offences,
- companies incorporated in offshore jurisdictions,
- Businesses engaged in commercial activities involving nuclear products, except for duly authorised projects carried out in connection with government-funded investments,
- Shell Banks, other money service businesses or companies operating payable-through accounts or transit accounts,
- Individuals and companies engaged in trust management activities for the purpose of trust asset management (including management of trust assets/accounts), as well as businesses engaged in professional fiduciary asset management,
- Asset management foundations engaged in long-term wealth management,

- The Bank establishes business relationships with private investment funds only in exceptional cases and subject to strict controls, provided that such a relationship does not conflict with the Bank's interest in protecting its reputation.

High-Risk Factors Assessed During the Establishment and Maintenance of a Business Relationship

When establishing or maintaining a business relationship, the MagNet Bank considers the following factors to present a higher risk and, in all cases, conducts a separate expert Anti-Money Laundering (AML) assessment before deciding whether to establish or continue the relationship:

- Labour-intensive businesses, as well as companies operating in the construction industry, pharmaceutical and healthcare sectors, defence industry, mining industry, and public procurement sector;
- Businesses involved in payment services, casino operations, or precious metals trading;
- Businesses with high volumes of cash transactions;
- Individuals or companies that have been the subject of adverse media or other relevant negative information (e.g. allegations or evidence relating to criminal activity or terrorism);
- Companies involving Politically Exposed Persons (PEPs), as well as non-profit organisations subject to applicable legal regulations;
- Non-resident legal entities and individuals as defined in the MagNet Bank's internal regulations who are unable to provide sufficient reason for using the MagNet Bank's services.

The following characteristics are also considered high risk and therefore subject to enhanced due diligence:

- Politically Exposed Persons (PEPs), including family members and close associates of PEPs;
- Non-face-to-face account opening (excluding account opening through the Magnet Bank's Video Banking service).

Regulatory Compliance

In accordance with applicable European Union regulations governing mandatory information requirements for funds transfers, it is essential that customers provide complete and accurate information regarding themselves, the beneficiaries of their outgoing transfers, and any other transactions recorded on their accounts.

Customers are advised that the MagNet Bank may request additional information or documentation concerning specific transactions or payment instructions, either before accepting a transaction or after it has been executed. The MagNet Bank reserves the right to reject certain transactions following a review and assessment.

Monitoring of Business Activity and Detection of Unusual or Prohibited Transactions

The Bank's Anti-Money Laundering, Sanctions Compliance, Counter-Proliferation Financing and Anti-Corruption procedures include monitoring programmes designed to identify unusual and prohibited transactions. For transactions flagged by these monitoring systems, the Bank may request additional information from customers regarding their account activity and transaction counterparties. If satisfactory responses are not received within a reasonable period of time, or if the nature and purpose of the business relationship cannot be reasonably justified to the Bank's satisfaction, the Bank reserves the right to reject certain transactions and, where necessary, immediately terminate the business relationship.

Sanctions Risk Appetite

The Bank does not establish or maintain business relationships with any natural or legal person appearing on any of the sanctions lists set out below or where such a relationship would otherwise be prohibited by law or regulation. The Bank will also not process any transaction involving such persons or entities.

The relevant sanctions lists include:

- The United Nations Security Council Sanctions Lists (UN);
- The Consolidated Financial Sanctions List of the European Union (EU);
- The sanctions lists administered by the United States Office of Foreign Assets Control (OFAC), including the Specially Designated Nationals and Blocked Persons List (SDN List).

The Bank applies screening and control procedures throughout its business processes to ensure full compliance with applicable legal requirements, sanctions restrictions, and, where these impose stricter requirements, the Bank's own internal policies and procedures.

From a risk perspective, the Bank also considers jurisdictions identified as tax havens, offshore jurisdictions, or countries presenting elevated risks relating to corruption, money laundering, or fraud to be high-risk countries. Such lists are compiled based on international standards and the Bank's own risk appetite framework.

Accordingly, before processing certain transactions or payment operations, the Bank may request additional information and documentation from customers regarding the transaction and the business partners involved. This requirement commonly applies to transactions involving former Soviet republics, high-risk third countries, and offshore jurisdictions.

The Bank will not process any transaction that involves a sanctioned person or entity, violates applicable sanctions, conflicts with the Bank's internal policies and procedures, or compromises the Bank's business relationships.

Restricted Countries and Transactions

Based on the principles outlined above, the Bank does not execute transactions that are directly or indirectly related to:

- Iran, Myanmar (Burma), North Korea, Sudan, South Sudan, Syria, or transactions involving the Ukrainian regions of Crimea, Luhansk, Donetsk, Zaporizhzhia, and Kherson;
- Transactions originating from, destined for, or otherwise connected with Russia or Belarus;
- Transactions involving Afghanistan, Cuba, Venezuela, or Yemen where the underlying activity or transaction is settled in U.S. dollars (transactions in other currencies are subject to individual review).

Based on its own risk assessment, the Bank also does not process transactions originating from or destined for the following countries and territories:

Algeria, Angola, Barbados, Burkina Faso, Burundi, Bolivia, Belarus, Congo, Central African Republic, Côte d'Ivoire (Ivory Coast), Eritrea, Ethiopia, Equatorial Guinea, Guinea-Bissau, Haiti, Iraq, Iran, Cameroon, Kenya, Democratic People's Republic of Korea (North Korea), Lao People's Democratic Republic (Laos), Lebanon, Libya, Moldova, Mali, Myanmar, Mozambique, Namibia, New Caledonia, Niger, Nigeria, Nicaragua, Nepal, Panama, Palestine, West Bank, Russia, Rwanda, Sudan, Senegal, Somalia, South Sudan, Syria, Chad, Trinidad and Tobago, Tanzania, British Virgin Islands, Vanuatu

Exceptions to the above restrictions may only be granted by the Bank in exceptional circumstances (e.g. where required by law, regulatory authority approval, or official order) and only following a detailed review and assessment.

The Bank reserves the right to update and amend the above lists from time to time.

Please also note that correspondent banks may, based on their own internal policies and procedures, decide to suspend, reject, return, or block any transaction. Such decisions are outside the control of the Bank.