Remote identification for the investors of the mutual funds managed by Signet Asset Management Latvia IPS

In accordance with the regulatory enactments in force in Latvia and the European Union, Signet Asset Management Latvia IPS (hereinafter — the Company) is required to identify its investors before every transaction with the investment certificates. Investor identification is necessary to verify the identity of investor and the ultimate beneficial owner of the transaction, to prevent the use of the financial system for illegal activities, and to comply with national and international sanctions requirements.

Signet Bank AS ensures the identification of investors who are **clients of Signet Bank AS** and wish to carry out transactions with investment certificates of the mutual funds managed by the Company (hereinafter — the investment certificates).

For investors who **are not clients of Signet Bank AS** and wish to carry out transactions with investment certificates, the Company provides remote identification in accordance with the procedure set out below:

1. What is remote identification?

Remote identification is the process by which the Company verifies an investor's identity. The Company carries out remote identification using a **secure electronic signature**[1] technology solution:

- the eParaksts service provided by VAS "Latvijas Valsts radio un televīzijas centrs" (LVRTC) (information available at https://www.eparaksts.lv) or
- an electronic signature provided by qualified trust service providers from other European Union Member States (list available on the eIDAS Dashboard https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls).

2. What is the remote identification process?

Remote identification using a secure electronic signature means that the investor must sign all documents to be submitted to the Company with a secure electronic signature and send the signed documents to the email address funds@signetam.com, which is used for correspondence with the Company.

The company requests to sign the documents in the following formats:

- documents signed using the eParaksts solution — in eDOC or ASICE format;
- documents signed using a secure e-signature issued in another EU Member State — in ASICE format;
- PDF files using the eDOC format (this option can be selected when signing the document on the eParaksts.lv portal or in the eParakstītājs software).

3. Who has access to remote identification?

Remote identification is available only to **clients of credit institutions registered in Latvia**:

- natural persons who are residents of Latvia or other EU Member States;
- legal entities registered in Latvia or another EU Member State whose ultimate beneficial owners, officials, representatives, shareholders, or members are residents of Latvia or other EU Member States.

The Company provides remote identification for investors who wish to carry out transactions with investment certificates, but **are not clients of Signet Bank AS.** The Company identifies such investors before every transaction with the investment certificates.

4. What services are available?

An investor identified by a secure electronic signature has access to transactions with the investment certificates of the mutual funds managed by the Company.

[1] In accordance with Article 1(2) of the Electronic Documents Law: a secure electronic signature is a qualified electronic signature within the meaning of Article 3(12) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter referred to as Regulation No 910/2014/EU).

5. What are the investor's obligations?

It is the investor's obligation to submit all information and documents requested by the Company within the specified time.

The investor (or their representative) has the following obligations:

- ensure that electronic signature creation data is not used by another person;
- immediately request a trusted certification service provider to revoke a qualified certificate or suspend its operation if there are grounds to believe that the electronic signature creation data has been used without the holder's knowledge;
- immediately request a trusted certification service provider to revoke a qualified certificate if the information contained therein changes.

The investor is required to ensure that the submitted documents comply with the requirements established by the Company. The documents to be submitted and the applicable requirements are available on the Company's website.

The following general requirements apply to copies of identification documents:

- the quality of the copy must reflect the same clearly understandable and unambiguously perceptible information as contained in the original document;
- all pages of the document containing text and other graphic information (e.g., information regarding the person's registered place of residence, spouse, and children) must be copied;
- when preparing a copy of a passport, it is permissible to copy only specific spreads (two passport pages on a single sheet of the copy), provided that the passport pages containing the person's photograph, personal and document details, and visas are included;
- it is preferable for the size of the copy to match the size of the original document.

6. Points to consider?

The Company reserves the right not to perform remote identification of an investor and not to accept an application for purchase / redemption of the investment certificates if the Company considers that such method of remote identification is not applicable to the respective investor or representative for the purpose of receiving the service. For example, if:

- identifies circumstances indicating that remote identification is not commensurate with the money laundering and terrorist and proliferation financing risk associated with the investor/representative;
- identifies circumstances indicating insufficient security or suitability of the remote identification process, or the lack of veracity of the information obtained;
- a discrepancy was identified regarding the information obtained during the due diligence of the investor/representative.

The Company or the investor/representative may terminate any stage of the remote identification process at any time without providing a reason. In such cases, the Company will inform the party that the application purchase / redemption of the investment certificates is not being accepted.

In the case of a legal entity, remote identification is performed only for those representatives who will represent the investor in its transactions with the Company.

If an investor has multiple authorized persons entitled to jointly submit applications, documents, and other information to the Company, these must bear the signatures of all such authorized persons. All of the investor's authorized persons jointly sign the documents using a secure electronic signature in the digital environment.

The Company has the right to request the submission of any other additional information and/or documents. It is the investor's obligation to submit all information and/or documents requested by the Company within the specified timeframes.

During the remote identification process, the Company processes the investor's personal data to carry out the identification and due diligence of the natural person. The Company carries out remote identification and the processing of personal data in compliance with the requirements set out in the Regulations of Cabinet of Ministers No. 392 of 3 July 2018, "Procedures by which a Subject of the Law on the Prevention of Money Laundering and Terrorism and Proliferation Financing Performs Remote Customer Identification." Information regarding the processing of personal data and the Privacy Policy is available on the Company's website https://signetbank.com/en/personal-data-processing/.

The Company verifies the information submitted by the investor/representative against public registers and restricted databases to confirm the accuracy of the information, assess the investor's risk level, check for inclusion in sanctions lists and lists of politically exposed persons, and evaluate the feasibility of providing services to the investor.

7. Regulatory framework

Law on Electronic Documents of the Saeima of the Republic of Latvia, Chapter VII “Obligations and Liability of a Trusted Certification Service Provider and a Signatory”, Section 25 “Obligations and Liability of a Signatory”

(1) A signatory has the following obligations:

4) to ensure that electronic signature creation data are not used without the signatory’s knowledge;

5) to immediately request that a trusted certification service provider revoke a qualified certificate or suspend its operation if there are grounds to believe that electronic signature creation data have been used without the signatory’s knowledge;
6) to immediately request that a trusted certification service provider revoke a qualified certificate if the information contained therein changes.

(2) The signatory is liable for damage caused to a person who has reasonably relied on a qualified certificate if:
1) the signatory provides false information to a trusted certification service provider;
2) the signatory fails to exercise due care in protecting the electronic signature creation data against unauthorized use;
3) it can reasonably be considered that the electronic signature creation data had been used without the signatory's knowledge, yet the signatory failed to request the trusted certification service provider to revoke or suspend the qualified certificate.

Information prepared on: 01.07.2026.