Paysera LT, UAB
300060819
Pilaitės av. 16, LT 04352 Vilnius
www.paysera.lt
Registry data processor - VĮ Registru centras

Marijus Plančiūnas
CEO
Paysera LT, UAB
Pilaitės av. 16
Vilnius 04352
Lithuania

2025-04-15 No 2971/2025

Police and Border Guard Board

Director General

Pärnu mnt 139, 15060

Tallinn, Estonia

ppa@politsei.ee

SUBJECT: Application to get access to Estonian identity documents database

Dear Mr Belitšev,

We refer to the 14.09.2023 correspondence between Mrs Mary Piibeleht of the Estonian Police and Border Guard Board (the Police) and Mrs Ana Dalakishvili of the Lithuanian licensed e-money institution UAB "Paysera LT" regarding UAB "Paysera LT-s" access to Estonian X-tee services, particularly the Estonian identity documents database via an application programming interface (API). A copy of the referred correspondence is attached as Appendix 1 to this application.

On behalf of Paysera LT, UAB (hereinafter referred to as "Paysera"), we hereby initiate the procedure for signing a contract that will facilitate a secure and efficient exchange of data between the Paysera Identity Verification System and the Police and Border Guard Board to Identity documents database.

Paysera is a Lithuanian electronic money institution licensed by the Bank of Lithuania under License No. 1, issued on 27 September 2012. As evidenced by the information published on the website of the Estonian Financial Supervision and Resolution Authority (EFSRA), Paysera is authorized to provide cross-border services in Estonia. https://www.fi.ee/et/makseteenused/makseteenused/e-raha-asutused/ulepiirilised-e-raha-teenuste-pakkujad/uab-paysera-lt,

Paysera offers a comprehensive range of financial services to its clients in Estonia which include:

1. Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account
2. Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account
3. Execution of payment transactions, including transfers of funds on a payment account with the payment service provider
4. Execution of payment transactions where the funds are covered by a credit line for a payment service user
5. Issue of payment instruments specified in subsection 709 (8) of the Law of Obligations Act; acceptance of payment transactions
6. Money remittance
7. Payment initiation service
8. Account information service
9. Issuing, distribution and redemption of electronic money

More detailed information about our services can be found on our official website: https://www.paysera.com/v2/en/index.

1. **The legal grounds for using the service: a reference to the relevant legislation, section, and paragraph**

According to § 2, subsection 2 of the Estonian Money Laundering and Terrorist Financing Prevention Act (the AML Act) it applies to financial institutions. § 6, subsection 2(3) of the AML Act provides legal definition of the term

‘financial institution’ clarifying that for the purposes of the Act, ‘financial institution’ shall mean an e-money institution within the meaning of the Payment Institutions and E-money Institutions Act.

Therefore, as a financial institution conducting activities within Estonia, Paysera falls under the purview of the AML Act. Furthermore, pursuant to § 19, upon establishment of a business relationship or in case of specific operations (§ 19(2)), the obliged entity is required to apply customer due diligence measures.

Customer due diligence measures under § 20 include identifying the customer or any person engaged in an occasional transaction and verifying the information provided using reliable and independent sources, which may involve electronic identification tools and trust services for electronic transactions. The obliged entity must also identify and verify any representative acting on behalf of the customer or the person involved in the transaction, as well as confirm their right of representation. In addition, the beneficial owner must be identified, and appropriate steps must be taken to verify their identity, ensuring that the obliged entity has a clear understanding of who the beneficial owner is, along with the ownership and control structure of the customer or transaction participant.

In accordance with § 21 subsection 1, financial institutions must identify the customer or their representative by collecting specific data. This includes the person’s full name, their personal identification code, or—if such a code is not available—their date of birth and place of residence or location.

Additionally, the institution must obtain information necessary to recognise and verify the right of representation and its scope. Where the right of representation does not arise from law, the name of the document serving as the basis for that right, the date of its issue, and the name of the issuing authority must also be recorded. What is more, financial institutions must verify the correctness of the data specified in under § 21, subsection 1, clauses 1 and 2, using information originating from a credible and independent source for that purpose.

Pursuant to § 21 subsection 3, the identification of customers who are natural persons must be carried out using an appropriate set of documents. This includes a document specified in subsection 2 of § 2 of the Identity Documents Act, a valid travel document issued by a foreign country, or a driving licence that complies with the requirements set out in subsection 1 of § 4 of the Identity Documents Act. In the case of a person under the age of seven, identification may be conducted on the basis of a birth certificate as specified in § 30 of the Vital Statistics Registration Act.

Furthermore, according to § 31 (due diligence measures applied by financial institutions performing remote identification of persons) subsection 5 of the AML Act, to identify the person and verify data, the financial institutions may use personal identification data recorded in the database of identity documents.

Moreover, according to § 47 subsection 6, upon implementation of § 31 of the AML Act, the obliged entity retains the data of the document prescribed for the digital identification of a person, information on making an electronic enquiry to the identity documents database, and the audio and video recording of the procedure of identifying the person and verifying the person’s identity for at least five years after termination of the business relationship.

In accordance with § 48 subsection 1 the obliged entity must implement all rules of protection of personal data upon application of the requirements arising from the AML Act. Additionally, subsection 2 requires the obliged entity implement all rules of protection of personal data upon application of the requirements arising from the AML Act. This principle is aligned with the General Data Protection Regulation (GDPR), which mandates that processing must be lawful, transparent, and purpose-limited.

As this processing is necessary to comply with legal obligations imposed on Paysera as a data controller, it qualifies as lawful under Article 6(1)(c) GDPR. Furthermore, such processing is consistent with the data protection principles set forth in Regulation (EU) 2016/679, particularly regarding lawfulness, fairness, and purpose limitation.

In addition to the primary legal basis under Article 6(1)(c) GDPR, Paysera also relies on two supplementary legal grounds:

1. Customer consent under Article 6(1)(a) GDPR, as clients provide explicit consent during the onboarding process; and
2. Contractual necessity under Article 6(1)(b) GDPR, as personal data processing is essential to perform the General Payment Service Agreement between Paysera and its clients. This agreement sets out core obligations related to the provision of payment services, customer authentication, and transaction execution.

As a data controller, Paysera processes personal data in strict compliance with its publicly available Privacy Policy, which outlines all relevant rights and protections afforded to data subjects. For further information, please refer to: https://www.paysera.com/v2/en/personal-data-protection.

Paysera has appointed a Data Protection Officer to oversee compliance with data protection regulations, as outlined above.

Name: Justina Kučinskė
Email: dpo@paysera.com

2. **The purpose of using the service: the detailed work process in which the service is used**

The purpose of using the service is to fulfill the obligations arising from the Estonian Anti-Money Laundering Act regarding the application of due diligence measures, as well as to comply with the anti-money laundering policies of Paysera during the customer onboarding process. The service will be used for the following purposes:

Customer Identity Verification: The service will be used to verify the authenticity and validity of identification documents submitted by Estonian customers during the onboarding process.

Automated Check: The service is intended to be integrated into Paysera's system to automate the process of verifying the validity of identification documents. This automation will significantly enhance the efficiency and accuracy of identity verification.

Compliance: This service is essential for ensuring compliance with regulatory requirements, particularly those related to anti-money laundering (AML) and know-your-customer (KYC) obligations. The service will play a key role in ensuring that only legitimate customers are onboarded.

3. **The precise data that is needed (input and output data)**

The necessary input data comprises specific information extracted from the customer's identification document, including:

- Document number,
- Full name of the individual,
- Identification number,
- the date of birth, and
- the expiration date of the document.

This data is required to enable the verification process during customer onboarding.

The necessary output data consists of the validation result, which confirms whether the submitted identification document is authentic, valid, and matches the personal information provided by the customer.

4. **The service volume: how many requests are planned in a set time period (i.e. per calendar month).**

The anticipated volume of identity document validation requests is estimated at approximately 600 verification requests per calendar month.

We would appreciate it if you could inform us whether you have any questions or require additional clarification regarding the above information. Additionally, we kindly request an indication of the expected timeline within which a positive decision may be made concerning the granting of access for Paysera to the Estonian identity documents database via API.

Furthermore, we look forward to receiving the draft version of the data exchange agreement concerning the above-mentioned integration. This agreement should define the precise input and output data fields, as well as any additional technical or procedural requirements applicable to the data exchange.

We also look forward to receiving the draft data exchange agreement concerning this matter, which is expected to specify the exact input and output data fields, along with any other applicable technical and procedural requirements.

Contact details:
Contact person for contractual issues: Grisha Dimitrov
Email: grisha.ivanov@paysera.net.

Contact person for technical issues: Petar Minkov
Email: petar.minkov@paysera.net .

We appreciate your consideration of this request and look forward to your response. Should you need further clarification, please do not hesitate to contact me at marijus.planciunas@paysera.net.

Sincerely,
Marijus Plančiūnas
CEO, Paysera LT, UAB

Appendix 1: Expanded extract from the Register of Legal Entities of the Republic of Lithuania