

NARVI PAYMENTS PRIVACY NOTICE

We process your personal data for the following purposes as a controller:

- Provision of EMI services
- KYC (Know Your Customer)
- Communications

This notice concerns the payment and electronic money services provided by Narvi Payments Oy Ab. It explains how we use personal data about customers, their representatives and beneficial owners, payment counterparties and people who contact us.

1 OUR INFORMATION

Contact information:

The controller for the processing described in this notice is Narvi Payments Oy Ab (business ID 3190214-6).

Our contact address is Maria 01, Lapinlahdenkatu 16, 00180 Helsinki, Finland.

For privacy questions and requests to exercise your rights, contact contact@narvi.com.

Operations-related information:

Narvi Payments Oy Ab is an electronic money institution supervised by the Finnish Financial Supervisory Authority (FIN-FSA).

Information about our authorisation is available in the FIN-FSA register of supervised entities.

2 KEY TERMS AND REGULATIONS

Act on Payment Institutions (297/2010) is the law that governs businesses involving payment services.

Act on Payment Services (290/2010) is the law that governs the obligation to provide information, terms of contracts, and implementation related to payment services.

Act on Preventing Money Laundering and Terrorist Financing (444/2017) is the law that governs the prevention, detection, and investigation of money laundering and terrorist financing—also referred to as the AML Act hereinafter.

Controller means the party responsible for processing the data subject's personal data.

The people covered by this notice include individual customers; representatives, contact persons and beneficial owners of business customers; persons connected with payment transactions; and people who contact us.

Data subject is a term for a human being in accordance with data protection laws.

DPO is a term for an independent representative of a controller or a processor who helps the controller or the processor ensure that it complies with relevant data protection laws.

EMI means an electronic money institution authorised under the Finnish Act on Payment Institutions (297/2010).

KYC (Know Your Customer) means verifying the customer's identity, ascertaining the customer and his/her assets and backgrounds, and knowing and following the behavior that is characteristic of the customer.

The legal basis for processing means the legal ground on which the controller processes the data subject's data. The lawfulness of processing is described in Article 6 of the EU Data Protection Regulation.

Personal data means any information concerning the data subject or information by which the data subject can be identified

Privacy Notice means a document drawn up in accordance with Articles 13 and 14 of the EU Data Protection Regulation through which the controller informs data subjects of the ways their personal data is processed.

Purpose for processing means the reason why the controller processes the data subject's personal data.

3 WHY DO WE PROCESS YOUR PERSONAL DATA?

We process your personal data in accordance with the processing purposes listed below. In the sections, you will find information on what personal data we process and for what legal basis we process your personal data.

Provision of EMI services

We process data to open and operate accounts, issue electronic money, execute and receive payments, provide customer support and administer our services. This includes information about customers, their representatives and payment counterparties.

Categories of personal data: identity and contact details, account and payment details, transaction records, instructions, correspondence and technical information needed to provide and secure the service.

Legal bases under Article 6(1) GDPR: performance of a contract with an individual customer or steps requested before that contract (point (b)); compliance with applicable payment, recordkeeping and regulatory duties (point (c)); and our legitimate interests in providing and securing services to business customers and handling operational queries (point (f)), where those interests are not overridden by the individual's rights. Any express consent required under payment-services rules is distinct from consent as a GDPR legal basis.

Customer due diligence, sanctions screening and financial crime prevention

We identify and verify customers, representatives and beneficial owners; assess risk; screen relevant parties; monitor transactions; investigate unusual activity; and make reports where required by law.

Categories of personal data: identity and contact details, identifiers and identity documents, tax residency and identification details where required, ownership and control information, occupation and business information, source of funds or wealth where relevant, screening results, transaction information and investigation records.

Legal basis: compliance with legal obligations, including the Finnish Act on Preventing Money Laundering and Terrorist Financing (444/2017), applicable sanctions obligations and other relevant financial-sector duties (Article 6(1)(c) GDPR). Fraud prevention and the security of our services may also rely on our legitimate interests where applicable (Article 6(1)(f)).

Communications

Explanation: Personal data is processed to carry out communications. Category of data subjects: People who contact us.

Categories of personal data: your contact details and the contents of your communication. Legal basis: our legitimate interest in responding to enquiries and managing business communications (Article 6(1)(f) GDPR); where the enquiry concerns steps requested before entering into a contract with you, Article 6(1)(b) may apply.

If processing is based on our legitimate interests, you may object on grounds relating to your particular situation, subject to the conditions in Article 21 GDPR.

4 FROM WHERE DO WE COLLECT YOUR PERSONAL DATA?

We collect your personal data from different sources. The sources of information we use depend on our processing purposes.

Provision of our services and KYC

We collect your personal data from yourself, our business partners, authorities, and different public sources, such as the trade register.

As customer identification and knowledge is a prerequisite for our business, we utilize personal data about you provided by third parties, such as information provided by identification services and sanction list providers.

Communications

We collect your personal data from you.

5 DO WE TRANSFER YOUR PERSONAL DATA?

We disclose personal data where needed to deliver our services or meet legal obligations, including to payment systems, correspondent and partner banks, service providers acting for us, professional advisers and competent authorities. We apply appropriate contractual and security safeguards.

Where personal data are transferred outside the European Economic Area, we rely on an applicable adequacy decision or appropriate safeguards, such as European Commission standard contractual clauses, and take supplementary measures where required. You may request information about the relevant safeguards through the contact address above.

Personal data may be transferred to the following third parties:

- Recipients may include hosting, IT, communications and customer support providers; payment infrastructure and banking partners; identity verification, screening and fraud prevention providers; and public authorities where disclosure is required or permitted by law.

6 HOW LONG DO WE RETAIN YOUR PERSONAL DATA?

We keep personal data only for as long as necessary for the purposes described above, subject to applicable statutory retention requirements. We review retention periods and delete or anonymise data when the applicable period ends, unless another lawful reason requires continued retention.

Services and customer due diligence

Customer due diligence information is generally kept for five years after the end of the regular customer relationship or, for occasional transactions, five years after the transaction, under the Finnish AML Act. Longer retention is limited to cases permitted or required by applicable law, such as an ongoing criminal investigation or legal proceedings.

Payment and accounting records are retained for the periods required by the applicable payment, accounting and other laws. The precise period depends on the record and the relevant legal requirement.

Communications

We generally keep routine enquiries for up to three years after the last contact, unless the matter forms part of a customer record, dispute or legal claim that requires a different period. Website cookies are described separately in our cookie information, where applicable.

7 WHAT DATA PROTECTION RIGHTS DO YOU HAVE?

You may exercise your rights by contacting us at contact@narvi.com. We may ask for information reasonably needed to verify your identity. The scope of a right depends on the applicable legal basis and any statutory restrictions, including restrictions concerning certain AML records.

You may lodge a complaint with the Finnish Data Protection Ombudsman (tietosuoja.fi) or another competent data protection supervisory authority.

Right of access

You may request confirmation of whether we process your personal data and access to those data, subject to applicable restrictions.

Rectification and erasure

You may request correction of inaccurate data and erasure where the conditions under the GDPR are met. We may need to keep data to comply with a legal obligation or establish, exercise or defend legal claims.

Restriction of processing

You may request restriction of processing where the conditions under the GDPR are met.

Data portability

Where processing is automated and based on consent or a contract, you may request the personal data you provided to us in a structured, commonly used, machine-readable format and, where technically feasible, its transmission to another controller.

Right to object

You may object at any time to processing for direct marketing, including related profiling. We will then stop processing your data for that purpose.

Where we rely on legitimate interests, you may object on grounds relating to your particular situation. We will stop processing unless we demonstrate compelling legitimate grounds or the processing is needed for legal claims.

Automated individual decision making

If we make a decision based solely on automated processing that produces legal or similarly significant effects, we will provide the information and safeguards required by Articles 13 to 15 and 22 GDPR.

Withdrawal of consent

Where we rely on GDPR consent for a specific activity, you may withdraw it at any time without affecting processing carried out before withdrawal. The activities described above do not generally rely on GDPR consent.

8 CAN THIS PRIVACY NOTICE BE AMENDED?

We may update this notice when our processing or legal requirements change. We will publish the current version and, where required, bring material changes to affected people's attention.

Last updated 28 September 2026