

## **NARVI AND NV EXCHANGE PRIVACY NOTICE**

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

- a) Provision of EMI services
- b) Provision of crypto-asset services
- c) KYC (Know Your Customer)
- d) Communications

Please note that this Privacy Notice contains information on both Narvi's EMI services and NV Exchange's crypto-asset services since the services are provided in unison – despite the fact that the services are provided by different companies.

### **1) OUR INFORMATION**

#### Contact information:

The controller of your personal data in connection to:

- EMI services is Narvi Payments Oy Ab (business ID: 3190214-6), and
- crypto-asset services in NV Exchange Ab (business ID: 3316814-1).

Both companies are located at Maria 01 Lapinlahdenkatu  
16, 00180 Helsinki.

We have appointed a DPO, whom you can contact via  
email at: [privacy@narvipay.com](mailto:privacy@narvipay.com).

#### Operations-related information:

Both Narvi Payments and NV Exchange operate under the supervision of the Finnish Financial Supervisory Authority (FSA):

- Narvi Payments is an E-money Institution (EMI) operating based on a license issued by the FSA, and
- NV Exchange is a Virtual Asset Service Provider (VASP) operating based on a registration issued by the FSA.

You can find more information about the controller's EMI license and VASP registration from the FSA's [list](#) 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.

Act on Virtual Currency Providers (572/2019) is the law that governs VASPs.

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

Customer means our customers, the persons who execute payment transactions with our customers, the politically influential persons (so-called PEPs) associated with them, and the actual beneficiaries. In addition, in the case of a legal entity, the customer also means the contact persons of the legal entity.

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 is a licensed electronic money institution under the Act of 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.

#### a) Provision of EMI services

Explanation: Personal data is processed to provide EMI services to our customers. Category of data subjects: Customers.

Categories of personal data: Contact details, payment account information, bank details, and data related to the use of payment services.

Legal basis for processing: According to Section 86 of the Act on Payment Services of Finland (290/2010), the legal basis for processing is consent.

#### b) Provision of crypto-asset services

Explanation: Personal data is processed to provide crypto-asset services to our customers.

Category of data subjects: Customers.

Categories of personal data: Contact details, payment account information,

bank details, and data related to the use of crypto-asset services.

Legal basis for processing: Performance of our contractual obligations with the Customers.

#### c) KYC (Knowing Your Customer)

Explanation: Personal data is processed to identify and know our customers.

Category of data subjects: Customers.

Categories of personal data: Personal data as required by law, such as personal identification numbers, purposes, and methods of use of the service, ownership relationships, the quality and scope of the business of the customer, and the customer's beneficial owner.

Legal basis for processing: Our statutory obligations under the Act on Preventing Money Laundering and Terrorist Financing of Finland (444/2017).

#### d) Communications

Explanation: Personal data is processed to carry out communications.

Category of data subjects: People who contact us.

Categories of personal data: Contact details and possibly other data disclosed to us by the data subject. Legal basis for processing: Our legitimate interests, according to which we communicate. Our interests align with those of the people who contact us, as they expect us to process their data for communications purposes.

*NB! You may have a right to object to data processing for these purposes (see the section concerning your rights).*

### 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.

#### a) – b) Provision of our services and c) 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 prerequisites for our business, we utilize personal data about you provided by third parties, such as information provided by identification services and sanction list providers.

#### d) Communications

We collect your personal data from you.

#### 5) DO WE TRANSFER YOUR PERSONAL DATA?

We may transfer personal data to third parties as a normal course of our business. When personal data is transferred to third parties, we ensure that the transfers are carried out securely and in accordance with adequate data protection agreements.

We may also transfer personal data to third countries. When doing so, we ensure an adequate level of data protection, e.g., by using standard contractual clauses issued by the European Commission and other similar arrangements.

Personal data may be transferred to the following third parties:

- All personal data may be transferred to data storage, and communications services providers
- Data related to the use of our services may be transferred to third parties that provide KYC services to us.
- Accounting-related data may be transferred to financial management services

#### 6) HOW LONG DO WE RETAIN YOUR PERSONAL DATA?

The retention period of your personal data depends on the purposes for which we process your personal data. We inspect the necessity of the personal data stored regularly and keep records of the inspections.

a) – b) Provision of our services and c) KYC

We retain the necessary personal data for as long as it is required by law and our industry.

We will retain your customer information for at least five (5) years after the end of your customer relationship, and longer if necessary, e.g. to resolve a criminal case.

We retain data related to transactions and assignments for five (5) years, and the data will be retained by us for five (5) years after the end of the customer relationship.

We retain personal data related to the prevention and combating of money laundering, terrorist financing and fraud for at least five (5) years after the end of the customer relationship.

c) Communications

We will retain the necessary personal data for three (3) years after the contact. We retain social media information until individuals remove their information from our social media channels. Cookies: the retention period depends on each cookie used.

## 7) WHAT DATA PROTECTION RIGHTS DO YOU HAVE?

You may have the right to use the below listed data protection rights. The contacts concerning the rights shall be submitted to the controller's contact person. Your rights can be put into action only when you have been satisfactorily identified.

You may also have a right to complain to the supervisory authority if you think your data's processing infringes the data protection laws.

### Right to inspect

The data subject has a right to inspect what data the controller has stored of him/her.

### Right to rectify and erasure

The data subject has a right to request the controller to rectify or erase the personal data concerning the data subject on the grounds provided by law.

### Right to restriction of processing

The data subject can request the controller to restrict the processing of the personal data concerning the data subject on the grounds provided by law.

### Right to data portability

The data subject shall have a right to receive the personal data concerning him/her, which he/she has provided to the controller, in a structured, commonly used and machine-readable format where the processing is performed automatically and based on consent or a contract.

### Right to object

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him/her for such marketing.

Where personal data are processed on the basis of the legitimate interests of the controller, the data subject shall have the right to object the processing of personal data concerning him/her for such purposes in accordance with the law.

### Automated individual decision-making, including profiling

The data subject shall have a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her or similarly significantly affects him/her.

## Right to withdraw consent

Where the legal basis for the processing of personal data is the consent of the data subject, the data subject shall have the right to withdraw his/her consent.

### 8) CAN THIS PRIVACY NOTICE BE AMENDED?

We may unilaterally amend this Privacy Notice. We update the Privacy Notice as necessary, for example, when there is a change in legislation. Amendments to this privacy notice will take effect immediately when we post an updated version on our website.

If we make significant changes to the Privacy Notice, or if there is a significant change in the way it is used, we will notify the data subjects.

(Last update 19.4.2024)