

PRIVACY POLICY

NexNurture s.r.o., operating as Newrails

Effective from: May 18, 2026

1. Introduction and scope

This Privacy Policy ("Policy") describes how NexNurture s.r.o., Company ID 222 98 126, with its registered seat at Rohanské nábřeží 678/23, Karlín, 186 00 Praha 8, Czech Republic ("Company", "we", "us") processes personal data in connection with the provision of USDC custody and exchange services through the Newrails platform.

The Company is a data controller within the meaning of Regulation (EU) 2016/679 ("GDPR") and Act No. 110/2019 Coll., on the Processing of Personal Data.

This Policy applies to personal data of the Company's clients and their representatives in connection with the VASP services described in the NexNurture s.r.o. Terms and Conditions. It does not apply to services provided by Newrails UAB — those are governed by the Newrails UAB Privacy Policy.

Contact for personal data matters: cz.privacy@newrails.xyz

2. How we receive your personal data

We collect personal data in the following ways:

- Data you provide directly — when completing the USDC services questionnaire, accepting these Terms, providing proof of wallet ownership, or communicating with us
- Data received from Newrails UAB — under a Data Sharing Agreement, we receive KYB/KYC identification data, risk profile data, and account information collected by Newrails UAB during client onboarding and in the course of the business relationship
- Data generated through use of services — transaction records, wallet addresses, on-chain activity
- Data from third-party sources — blockchain analytics providers (for transaction screening and wallet risk assessment), public sanctions and PEP databases

3. Purposes, legal bases, and retention periods

We process personal data for the following purposes:

3.1. Provision of VASP services

Purpose	Providing EURW and USDC custody, EURW→USDC exchange, and USDC withdrawal services
Data subjects	Clients and their representatives
Personal data	Name, contact details, wallet addresses, transaction data, EURW and USDC balance data, USDC questionnaire responses, proof of ownership records, consent modal logs
Legal basis	Performance of a contract (GDPR Article 6(1)(b))
Retention	10 years after termination of the business relationship

3.2. AML/CFT and sanctions compliance

Purpose	Fulfilling obligations under Act No. 253/2008 Coll. (AML Act), including transaction monitoring, blockchain analytics screening, sanctions screening, and suspicious transaction reporting to FAU
Data subjects	Clients and their representatives
Personal data	Name, wallet addresses, transaction data, blockchain analytics screening results, PEP, sanctions and adverse media screening data, internal alert records and compliance decisions, STRs submitted to FAU
Legal basis	Legal obligation (GDPR Article 6(1)(c)); where special categories of data are processed (e.g. political beliefs of PEPs): GDPR Article 9(2)(g)
Retention	10 years after termination of the business relationship

3.3. Reporting to supervisory authorities

Purpose	Reporting to FAU (Czech Financial Analytical Office) as required by applicable law
Data subjects	Clients and their representatives
Personal data	All data necessary to fulfil reporting obligations, including identity data, transaction data, and AML/CFT records
Legal basis	Legal obligation (GDPR Article 6(1)(c))
Retention	10 years after termination of the business relationship

3.4. Travel Rule compliance

Purpose	Collecting, verifying, and transmitting originator and beneficiary information for virtual asset transfers in accordance with Regulation (EU) 2023/1113 (TFR)
Data subjects	Clients
Personal data	Name, wallet address, proof of ownership records
Legal basis	Legal obligation (GDPR Article 6(1)(c))
Retention	10 years after termination of the business relationship

3.5. Direct communication and complaints handling

Purpose	Responding to client enquiries, requests, and complaints
Data subjects	Clients and their representatives
Personal data	Name, contact details, communication content, transaction information
Legal basis	Legitimate interest of the Company in examining requests and providing accurate information (GDPR Article 6(1)(f))
Retention	3 years

3.6. Legal claims

Purpose	Establishing, exercising, or defending legal claims
Data subjects	Clients and their representatives
Personal data	All data relevant to the claim
Legal basis	Legitimate interest (GDPR Article 6(1)(f))
Retention	Until end of relevant legal proceedings and for a further 10 years

4. Data sharing and recipients

We may share your personal data with the following recipients:

- Newrails UAB — under a Data Sharing Agreement, for KYC/AML compliance and shared compliance services. Newrails UAB acts as a separate data controller for its own processing.
- FAU (Czech Financial Analytical Office) — mandatory reporting of suspicious transactions under the AML Act
- Blockchain analytics provider — for transaction screening and wallet risk assessment, acting as data processor under a data processing agreement.
- Courts, law enforcement, and other competent authorities — where required by law or court order
- Legal, audit, and professional service providers — where necessary for the Company's legitimate business operations

All personal data is processed within the EU/EEA. Where data is transferred outside the EU/EEA, appropriate safeguards under Chapter V of GDPR are applied.

5. Security of personal data

The Company implements appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, alteration, disclosure, and other unlawful processing. These include:

- Encryption of personal data at rest and in transit
- Role-based access controls and multi-factor authentication
- Regular security assessments
- Data minimisation — we process only data that is necessary for the specified purposes

While we strive to protect your data, no method of transmission or storage is completely secure. In the event of a personal data breach, we will notify the relevant supervisory authority and affected data subjects in accordance with GDPR requirements.

6. Your rights

As a data subject, you have the following rights under GDPR:

- Right of access — you may request confirmation of whether we process your personal data and, if so, access to that data
- Right to rectification — you may request correction of inaccurate or incomplete data

- Right to erasure — you may request deletion of your data where there is no legal basis for continued processing. Note: this right is limited where we are required by law to retain data (e.g. AML Act retention obligations)
- Right to restriction of processing — you may request that we restrict processing of your data in certain circumstances
- Right to data portability — where processing is based on contract or consent and carried out by automated means
- Right to object — you may object to processing based on legitimate interests

To exercise your rights, please contact us at: cz.privacy@newrails.xyz Your request must include your name, company name, and contact details. We will respond within 30 calendar days. In complex cases, this may be extended by a further 60 days with prior notice.

You have the right to lodge a complaint with the Czech supervisory authority: Úřad pro ochranu osobních údajů (UOOU), www.uouu.cz. We recommend contacting us first to resolve any concerns.

7. Changes to this Policy

We may update this Policy from time to time to reflect changes in our services, applicable law, or data processing practices. We will notify you of material changes through the Platform or by email. The updated Policy will be effective from the date of publication.

NexNurture s.r.o., operating as Newrails

IČO: 222 98 126 | Rohanské nábřeží 678/23, Karlín, 186 00 Praha 8

Privacy contact: cz.privacy@newrails.xyz | Web: newrails.xyz