

ECNG DIGITAL Sp. z o. o.

116/52 Piotrkowska 90-006 Łódź, Republic of Poland

NIP (TIN): 7252346635

REGON (Statistical Number): 52959293300000

KRS (Commercial Number): 0001125801



Registered in the VASP register under number RDWW-1529 (27.09.2024)

ECNG Digital sp. z o. o. is subject to supervision by: the General Inspector of Financial Information (GIIF) in the area of counteracting money laundering and terrorist financing. Contact details for GIIF:

<https://www.gov.pl/web/finanse/generalny-inspektor-informacji-finansowej>

Privacy Policy

ECNG Group

Last revised: 22 December 2025

1 WHO WE ARE – JOINT CONTROLLERS

Entity	Role	Registered address	Company No.
ECNG Digital Sp. z o.o.	Primary controller for customer accounts	ul. Piotrkowska 116/52, 90-006 Łódź, Poland	7252346635
ECNG Digital UAB	Legacy retention controller	A. Goštauto g. 8-143, LT-01108 Vilnius, Lithuania	305940403
ECNG Int OÜ	Strategy, licensing	Vaksali tn 6-1, Tartu 50409, Estonia	14438674
ECNG Labs OÜ	R&D, analytics	Vaksali tn 6-1, Tartu 50409, Estonia	16857435

All four companies jointly determine the purposes and means of processing ("joint controllers" within the meaning of Art 26 GDPR), jointly and severally, shall be referred to as "us", "we", "our/s").

We respect the privacy of our customers (each, "you" or "Customer") and are committed to protecting the privacy of Customers who access, visit, use or engage with our website or any other online services we provide (collectively the "Services").

From 22 December 2025, ECNG Digital Sp. z o.o. is the primary controller for customer accounts and day-to-day service operations.

ECNG Digital UAB continues to process and store certain customer records as an independent controller where this is necessary to comply with Lithuanian legal retention obligations (e.g., AML/CTF record-keeping), even after your account relationship is migrated.

We have prepared this Privacy Policy to outline our practices with respect to collecting, using, and disclosing your information when you use the Services.

We encourage you to read the Privacy Policy carefully and use it to make informed decisions. By using the Services, you agree to the terms of this Privacy Policy and your continued use of the Services constitutes your ongoing agreement to the Privacy Policy.

The Privacy Policy is a part of the Terms of Service available at <https://files.ecng.digital/cdn/policy/tos> and is incorporated herein by reference.

For the avoidance of doubt, capitalized terms not defined in this Privacy Policy have the meanings given in the Terms of Service.

In this Privacy Policy you will read about, among other things:

- Essence of our joint-controller arrangement;
- Why and what type of information we collect and our legal basis for its collection;
- Legitimate interests – how we balance them against your rights;
- Is the information obligatory? What happens if you refuse to share it?
- How we use the information;
- Automated decision-making and profiling;
- With whom we share the information and for what purpose;
- International transfer;
- Your privacy rights;
- For how long we retain the information;
- How we protect your information;
- Marketing;
- Minors;
- How to contact us.

Contact for all privacy matters

E-mail: dpo@ecng.digital

Legacy record retention by ECNG Digital UAB (Lithuania)

Following the migration of customer accounts and VASP operations on 22 December 2025, ECNG Digital UAB (Lithuania) continues to process and store certain customer data as an independent data controller for the limited purposes described below. This processing is separate from the day-to-day provision of services, which is managed by ECNG Digital Sp. z o.o. (Poland) as the primary controller for customer accounts.

Why ECNG Digital UAB retains this data

ECNG Digital UAB retains and processes certain records to:

- comply with Lithuanian statutory record-keeping obligations, including anti-money laundering and counter-terrorist financing (AML/CTF) requirements;
- respond to lawful requests from competent authorities and regulators;
- perform compliance audits, investigations and internal controls required by law; and
- establish, exercise or defend legal claims where relevant.

What data is retained

The retained records may include (as applicable to your account and activity):

- transaction and account history, including transfers, deposits/withdrawals, and related metadata;
- AML/CTF compliance evidence, such as KYC and KYB files, identity and verification data, beneficial ownership information, screening results (sanctions/PEP/adverse media), risk assessments, monitoring outputs and KYT/transaction monitoring alerts;
- corporate documents and supporting documentation provided for KYB/beneficial ownership verification;
- customer communications and compliance case notes relating to onboarding, monitoring, investigations, reporting decisions and other compliance matters; and
- audit logs and other records necessary to demonstrate compliance with AML/CTF obligations.

Legal basis

ECNG Digital UAB processes this legacy data primarily because it is necessary for compliance with a legal obligation (GDPR Article 6(1)(c)), including AML/CTF record-keeping requirements under Lithuanian law. Where applicable, processing may also be necessary for the purposes of substantial public interest in the area of AML/CTF or to meet regulatory requirements, and/or for the establishment, exercise or defence of legal claims.

How long the data is retained

ECNG Digital UAB retains the above records for 8 years from the end of the business relationship or the completion of the transaction (as applicable), in line with Lithuanian AML/CTF record-keeping requirements. In limited situations, retention may be extended if this is required or permitted by law (for example, where a competent authority lawfully requests an extension, or where records must be preserved for ongoing investigations or proceedings).

Your rights

You can exercise your data protection rights (including access, rectification, restriction, objection and, where applicable, erasure) by contacting dpo@ecng.digital

Please note that requests to delete or erase data may be restricted where ECNG Digital UAB must retain information to comply with legal obligations (such as AML/CTF record-keeping) or to establish, exercise or defend legal claims.

2 ESSENCE OF OUR JOINT-CONTROLLER ARRANGEMENT (Art 26 GDPR)

Task	Responsible entity	How this affects you
Transparency (privacy policy, in-app notices) Customer onboarding & KYC	ECNG Digital Sp. z o.o. ECNG Digital UAB (legacy record retention)	You receive one consolidated policy and set of notices. Shared databases; harmonised verification standards.
Day-to-day service operation	ECNG Digital Sp. z o.o.	Single point of contact for support.
R&D / risk analytics	ECNG Labs OÜ	Aggregated or pseudonymised data wherever possible.
Strategic management & regulatory liaison	ECNG Int OÜ	Ensures group-wide compliance and licence coverage.
Exercising your GDPR rights	Any ECNG entity (see §11)	You can submit a request to any office; we coordinate the response internally.
Information-security governance	All ECNG entities jointly	Digital Operational Resilience Act (“DORA”, Regulation (EU) 2022/2554): we apply its ICT-risk, incident-reporting and resilience-testing rules across the group.

3 WHY AND WHAT TYPE OF INFORMATION WE COLLECT AND OUR LEGAL BASIS FOR ITS COLLECTION

Why do you collect information about me?	Which information do you collect about me?	Why are you legally allowed to collect my information?	How long do you keep information about me?
1.1 To provide you with virtual currency exchange services, payment processing in virtual currencies services, when you are our customer	E-mail address, password, country, IP address, name and surname, sex, place of birth, address, telephone number, cryptocurrency address, bank account number, transaction amount, transaction currency, transaction time, address of the sender of the transaction, address of the payee of the transaction, ID number, ID copy, live video transmission, the image of your face and the original of the identity document shown by you are captured, power of attorney, data provided in business registration certificate, data provided in the document of business address proof, other information provided by you	We conclude and execute a service agreement with you (Art. 6 (1)(b) GDPR). Because we process your facial image for the purpose of uniquely identifying you, this constitutes biometric data and is also necessary for reasons of substantial public interest under Art. 9 (2)(g) GDPR, together with Art. 36 of the Polish AML Act	10 years after termination of your account
1.2 To implement measures of anti-money laundering (AML) and combating the financing of terrorism, including, but not limited to the proper identification of	Name and surname, personal (identity) code, date of birth, nationality, country of residence for tax purposes, country, postal code, address, telephone number, e-mail address, IP address, position, workplace city and state, sources of funds, jurisdictions from which funds are received and transferred,	We have legitimate interest (to prevent money laundering and terrorist financing) (Art. 6 (1) (c) of the GDPR) We must collect information according to the law for reasons of	10 years after the termination of business relations

sources of funds, sources of wealth	<p>planned turnover of services, services you use or plan to use, signature, risk level, the basis of representation.</p> <p>Participation in political activities, application of international financial sanctions and other restrictive measures.</p> <p>We also receive sanctions and politically-exposed-person information from Refinitiv World-Check One, ComplyAdvantage, the EU consolidated financial-sanctions list, the U.S. OFAC SDN list, Polish National Sanctions List, the United Nations Security Council Sanctions List (UN).</p>	substantial public interest (Art. 9 (2) (g) of GDPR)	
1.3 To inform you about our products and services that may be relevant to you	Name and surname, e-mail address	You agree that we will use information about you, or you purchased items or services from us. We have a legitimate interest (to provide service and product updates) (Art. 6 (1) (f) of GDPR)	10 years after the end of the customer relationship, unless you withdraw your consent
1.4 To handle queries, requests and complaints submitted by you	E-mail address, subject of your inquiry, date of your inquiry, content of your inquiry, attachments to your inquiry, your name and (or) surname provided in your inquiry, reply to your inquiry, information provided by you	We have a legitimate interest to do that (to handle your queries) (Art. 6 (1) (f) of the GDPR) Act on Consumer Rights in Poland and the Act of 5 August 2015 on the Handling of Complaints by Financial Market Entities, the Financial Ombudsman and the Financial Education Fund	10 years after the receipt of the last inquiry

1.5 To comply with legal requirements in the field of accounting when you are our customer, partner, or provider	Name, surname, e-mail address, telephone number, bank account number, address, signature, invoices, reports, accounting documents, payments, paid amounts, legal entity you represent	We have a legal obligation (we must collect information in accordance with the law) (Art. 6 (1) (c) of the GDPR) Tax law in Poland (incl. between others: Polish Accounting Act, Polish Tax Ordinance, Corporate Income Tax Act)	Within the time limits laid down by law
1.6 To ensure security of our website and continuously improve it for you	Internet protocol address (IP), referrer URL, date and time of website visiting	We have a legitimate interest (to ensure security of our website) (Art. 6 (1) (f) of the GDPR)	10 years after your last visit of our website
1.7 To engage in legal proceedings related to you	All information mentioned above, documents and attachments sent to you, documents and attachments submitted by you, procedural documents, court rulings, resolutions, decisions Information about criminal offenses and convictions	The processing is necessary for the establishment, exercise or defence of legal claims (Art. 6 (1)(f) GDPR). Because it involves data relating to criminal offences, we rely on Art. 10 GDPR	Within the time limits laid down by law

4 LEGITIMATE INTERESTS – HOW WE BALANCE THEM AGAINST YOUR RIGHTS

Whenever we rely on Article 6 (1)(f) GDPR ("legitimate interest") we have weighed our own objectives against your fundamental rights and expectations.

- For AML/risk-analytics our interest is to block illicit activity and comply with regulatory duties; the impact on you is limited to KYC checks that you would reasonably expect when using virtual-asset services.
- For website security our interest is to keep the platform safe; the data collected (IP address, time-stamp, referrer URL) is minimal and used only for intrusion detection.
- For direct marketing our interest is to grow our business by telling existing customers about similar products; you can object or opt-out at any time (see "Marketing").
- For handling queries and for defending legal claims our interest is to run our business efficiently and protect our rights; the processing is confined to the correspondence you send us.

We therefore believe that these interests are not overridden by your interests or fundamental rights and freedoms. You can always object to any processing based on legitimate interest (see "Your privacy rights").

5 IS THE INFORMATION OBLIGATORY? WHAT HAPPENS IF YOU REFUSE TO SHARE IT?

Certain data fields are statutory or contract-necessary:

- KYC/AML data – we cannot open or maintain an account without the identity and source-of-funds information required by Polish AML Act.
- Account credentials and contact details – without an e-mail address, password and country of residence we are unable to create a customer profile or provide the Services.
- Accounting data – accounting information must legally contain your name and address; refusing to provide them prevents us from proper billing and withholding fees for our services and therefore from delivering paid Services.

All other information is optional. If you choose not to give optional data (for example, optional marketing preferences), there will be no negative consequences other than not receiving the corresponding benefit (e.g. personalised offers).

6 HOW WE USE THE INFORMATION

We use and share your personal information in the manners described in this Privacy Policy. In addition to the purposes listed above, the information we collect, which may include your personal information, is used for the following purposes:

- To set up your account and to provide the Services;
- To identify and authenticate your access to certain features of the Services;
- To authenticate your identity for the purpose of compliance with regulatory (including AML) requirements;
- To communicate with you and to keep you informed of our latest updates;
- To market our website and the Services;

- To perform research or to conduct analytics in order to improve and customize the Services to your needs and interests;
- To support and troubleshoot the Services and to respond to your queries;
- To investigate and resolve disputes in connection with your use of the Services;
- To detect and prevent fraudulent and illegal activity or any other type of activity that may jeopardize or negatively affect the integrity of the Services; and
- To investigate violations and enforce our policies, and as required by law, regulation, or other governmental authority, or to comply with a subpoena or similar legal process or respond to a government request.

7 AUTOMATED DECISION-MAKING AND PROFILING

No fully automated decisions with legal or similarly significant effect are taken about you. We do, however, use automated risk-scoring tools to flag potentially suspicious transactions for manual review by our compliance team.

- Logic involved – the algorithm compares transaction patterns (amount, velocity, geo-location, blockchain heuristics) with known risk indicators published by FATF and local regulators.
- Consequences for you – a flagged transaction may be delayed while a human compliance officer checks the alert. You will be informed if additional information is needed or if the transaction is declined.
- Your rights – you may request human intervention, express your point of view, and contest the decision (Art 22 (3) GDPR).

8 WITH WHOM WE SHARE THE INFORMATION AND FOR WHAT PURPOSE

We do not rent, sell, or share your personal information with third parties except as described in this Privacy Policy.

We may share your personal information with the following recipients: (i) our subsidiaries; (ii) affiliated companies; (iii) subcontractors and other third-party service providers; (iv) auditors or advisers of our business processes; and (v) any potential purchasers or investors in the Legal entity.

In addition to the purposes listed in this Privacy Policy, we may share your personal information with our recipients for any of the following purposes: (i) storing or processing your personal information on our behalf (e.g., cloud computing service providers); (ii) processing such information to assist us with our business operations; (iii) performing research, technical diagnostics, personalization and analytics; and (iv) identity verification and fraud prevention services (AML service providers); and (v) communicating promotional and informational materials, in accordance with our marketing policy (see below under "Marketing"). These third-party service providers only have access to personal information needed to perform their functions but may not use it for other purposes. Further, they must process the personal information in accordance with our contractual agreements and only as permitted by applicable data protection laws.

We may also disclose your personal information or any information you submitted via the Services if we have a good faith belief that disclosure of such information is helpful or reasonably necessary to: (i) comply with any applicable law, regulation, legal process or governmental request; (ii) enforce our policies, including investigations of potential violations thereof; (iii) investigate, detect, prevent, or take action regarding illegal activities or other wrongdoing, suspected fraud or security issues; (iv) to establish or exercise our rights to defend against legal claims; (v) prevent harm to the rights, property

or safety of us, our affiliates, our Customers, yourself or any third party; (vi) for the purpose of collaborating with law enforcement agencies; and (vii) in case we find it necessary in order to enforce intellectual property or other legal rights.

You acknowledge that third party service providers may use your Personal Information or any information you submitted via the Services for analytics purposes, while ensuring that their processing of such information only results in anonymized and aggregated data.

As we continue to develop our business, we may share information, including your personal information, in the event of a corporate transaction (e.g., the sale of a substantial part of our business, a merger, de-merger, reorganization, consolidation of assets, the sale assets, or transfer of Services or part of Services thereof). In the event of the above, the acquiring company or transferee will assume the rights and obligations as described in this Privacy Policy.

9 THIRD PARTY COLLECTION OF INFORMATION

Our policy only addresses the use and disclosure of information we collect from you. To the extent that you disclose your information to other parties via the Services (e.g., by clicking on a link to any other website or location) or via other sites throughout the Internet, different rules may apply to their use or disclosure of the information you disclose to them.

You acknowledge that we are not responsible for the products, services, or descriptions of products or services that you receive from third party sites or to the content or privacy practices of those sites and that this Privacy Policy does not apply to any such third-party products and services. You are knowingly and voluntarily assuming all risks of using third party sites to purchase products and services. You agree that we shall have no liability whatsoever with respect to such third-party sites and your usage of them.

10 INTERNATIONAL TRANSFER

In most cases, personal data are processed and transferred in the territory of the European Union and the European Economic Area.

Limited transfers to service providers in the United States may occur. In such cases we rely on:

- the EU-U.S. Data Privacy Framework adequacy decision (10 July 2023), or
- the European Commission's 2021 Standard Contractual Clauses ("SCCs") plus a Transfer-Impact-Assessment and technical safeguards (encryption in transit and at rest, pseudonymisation).

You can request a copy of the Standard Contractual Clauses or a summary of the supplementary safeguards applied to a specific transfer by e-mailing dpo@ecng.digital. Confidential or commercially sensitive parts may be redacted.

11 YOUR PRIVACY RIGHTS

GDPR and other laws provide you with certain rights, procedures for implementation of and exceptions to these rights. When allowed by law, you can:

- Submit a request for confirmation that we are processing the data related to you. If we process the data related to you, request access to the data processed and related information;

- Submit a request to correct inaccurate or incorrect information used or to supplement it when it is not complete;
- Submit a request to delete the information we have about you if we use it illegally;
- Submit a request to restrict the processing of your personal information – if you dispute the accuracy of the data or object to the processing of the data, if you do not accept that your data would be deleted which was illegally processed, or if you need the data to claim, execute or defend legal claims;
- Object to collection, use and storage of your information by us – when we process data based on our legal and / or third party interests;
- Submit a request to transfer (receive) the data that you provided to us under the contract or giving the consent and which we process;
- To withdraw any consents given to us regarding information used about you - when we use the data based on your consent;
- Request human intervention and contest any automated decision that produces legal or similarly significant effects on you (Art. 22 (3) GDPR);
- To lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence or place of an alleged infringement of the GDPR and seek a judicial remedy.

If you have any questions or objection as to how we collect and process your personal information, please contact dpo@ecng.digital. All the requests will be fulfilled regarding GDPR 2016/679 clauses and will be answered within 30 days.

You may exercise your right to access your information, including account creating date, customer ID, your name, e-mail, phone, other profile information and transaction history in the "Profile" section of the platform. Using "Profile" section you can also exercise your right to revoke personal data or request personal data by clicking corresponding buttons.

Our lead supervisory authority is the Polish Data Protection Commissioner (UODO).

- Address: ul. Stanisława Moniuszki 1A, 00-014 Warsaw, Poland
- Tel.: +48 22 531 03 00 • E-mail: kancelaria@uodo.gov.pl • Website: <https://uodo.gov.pl/en/>

You can also complain to any other supervisory authority of the EU/EEA member state of your habitual residence or place of alleged infringement.

12 FOR HOW LONG WE RETAIN THE INFORMATION

We retain the information we collect for as long as needed to provide the Services (including aspects of risk management) and to comply with our legal and regulatory obligations, resolve disputes, and enforce our agreements (unless we are instructed otherwise). Retention periods will be determined taking into account the type of information that is collected and the purpose for which it is collected, bearing in mind the requirements applicable to the situation and the need to destroy outdated, unused information at the earliest reasonable time. Under applicable regulations, we will keep records containing account opening documents, communications, and anything else as required by applicable laws and regulations.

We may rectify, replenish, or remove incomplete or inaccurate information at any time and at our own discretion.

13 HOW WE PROTECT YOUR INFORMATION

We take great care of implementing and maintaining the security of the Services and your information. We aspire to continuously employ industry standard procedures and policies to ensure the safety of your information and prevent unauthorized use of any such information. Although we take reasonable steps to safeguard information, we cannot be responsible for the acts of those who gain unauthorized access or abuse the Services, and we make no warranty, express, implied, or otherwise, that we will manage to prevent such access.

Compliance with the Digital Operational Resilience Act (DORA) means we maintain a group-wide framework for ICT-risk management, continuous monitoring, penetration testing and 24-hour incident reporting to regulators. These sector-specific controls complement our GDPR obligation to implement appropriate technical and organisational measures to keep your data secure.

If you feel that your privacy was treated in discordance with our policy, or if any person attempted to abuse the Services or acted in an inappropriate manner, please contact us directly at dpo@ecng.digital

14 MARKETING

Your personal information, such as your full name, email address, etc., may be used by us, or by our third-party subcontractors to provide you with promotional materials concerning our Services.

Out of respect to your right to privacy, within such marketing materials, we provide you with means to decline receiving further marketing offers from us. In addition, at any time, you may request to unsubscribe and discontinue receiving marketing offers by sending us a blank message with the word "remove" to dpo@ecng.digital

Please note that even if you unsubscribe from our marketing mailing list, we may continue to send you service-related updates and notifications.

15 MINORS

The Services are not designated to individuals under the age of 18 or under legal age to form a binding contract under applicable laws. If you are under 18 years old or under legal age to form a binding contract under applicable laws, you should not use the Services or provide any personal information to us.

We reserve the right to access and verify any information collected from you. In the event that we become aware that an individual under the age of 18 or under legal age to form a binding contract under applicable laws has shared any of their information, we will discard such information. If you have any reason to believe that a minor has shared any information with us, please contact us at dpo@ecng.digital

16 COOKIES

We use cookies when you visit our website located at <https://ecng.digital> or any other websites, pages, features, or content we own or operate to operate and administer the website, conduct analytics and improve the website and your experience on it. For more information on our use of cookies, please see the Cookie Policy at <https://files.ecng.digital/cdn/policy/cookie>

17 UPDATES OR AMENDMENTS TO THE PRIVACY POLICY

We may revise this Privacy Policy from time to time, at our sole discretion, and the most current version will always be posted on our website at <https://ecng.digital>. In the event of a material change to the Privacy Policy, we may notify you through the Services or via email. We encourage you to review this Privacy Policy regularly for any changes.

Your continued use of the Services, following the notification of such amendments, constitutes your acknowledgment and consent of such amendments to the Privacy Policy and your agreement to be bound by the terms of such amendments.

18 HOW TO CONTACT US

If you have any general questions regarding the Services or the information that we collect about you and how we use it, please contact us at dpo@ecng.digital

19 INFORMATION ABOUT US

See §1