ECNG DIGITAL
ECNG privacy contact: dpo@ecng.digital

Privacy Policy

Effective: 1 July 2026

Simple summary. Your data is not automatically moved to Cornerstore. Cornerstore acts only for customers whose binding contractual relationship are validly novated and/or for customers who became customers starting 1 July 2026. ECNG Digital Sp. z o.o. and ECNG Digital UAB keep the records they must retain for their own legal and regulatory purposes. Migration to Cornerstore is optional. Only customers who explicitly choose to migrate and complete all required checks will become Novated Customers.

EU/EEA data-storage commitment. Cornerstore will store and retain all personal data transferred under this temporary arrangement, including backups and archive copies, only on servers located in the EU or EEA. It will not store, replicate or retain these data on servers outside the EU/EEA. Cornerstore acts as an independent controller under Costa Rican law (Ley 8968) and GDPR for EU/EEA data subjects. Cornerstore maintains all legally required database registrations, as required under Costa Rican law.

This policy explains how each company handles personal data during the temporary customer-by-customer transition. It is written in plain language, but it includes the information required by the GDPR.

1. Who is responsible for your data?

The controller is the company that decides why and how your personal data are used. The controller depends on your customer status and the records concerned.

Company	When it is the controller	Contact
ECNG Digital Sp. z o.o. Poland KRS 0001125801	Controller before an individual novation; controller for every Non-Novated Customer; and independent controller for its own historical, compliance, accounting, tax, audit, security, complaint and legal-claim records.	dpo@ecng.digital ul. Piotrkowska 116/52, 90-006 Lodz, Poland
ECNG Digital UAB Lithuania Company No. 305940403	Independent legacy-retention controller for records created before the 22 December 2025 migration from UAB to ECNG Digital Sp. z o.o.	dpo@ecng.digital A. Gostauto g. 8-143, LT-01108 Vilnius, Lithuania
Cornerstore Digital Limitada (Cornerstore) Costa Rica ID 3-102-962802	Separate, independent controller only after a customer has validly become a Novated Customer. It is responsible for the post-novation service, support, operational and compliance processing it carries out.	info@mycorner.digital Bufete Sanchez Chavarria, Costado Este de la Municipalidad de Garabito, Jaco 61101, Costa Rica

Cornerstore is not an ECNG Group company. ECNG Digital Sp. z o. o., ECNG Digital UAB and Cornerstore are separate controllers for their respective processing. ECNG Group companies and service providers may process data only where needed for a stated purpose and under the correct legal role. As Cornerstore is established outside the EU/EEA, Cornerstore will ensure the designation of an EU Representative for all processing activities involving EU/EEA data subjects.

2. What happens during the temporary transition?

The temporary arrangement started at 23:59 Warsaw time on 30 June 2026 and lasts for 90 calendar days, unless it is lawfully changed in writing. It is customer-by-customer, not a transfer of ECNG Digital Sp. z o.o.'s entire business or all customer records.

A customer becomes a Novated Customer only when:

- the customer has received the relevant terms and privacy information;
- Cornerstore has accepted the customer and completed the required AML, KYC, sanctions, risk and operational checks;
- the required record reconciliation and data-transfer safeguards are in place; and
- no legal, regulatory, compliance or security restriction prevents the transfer.

A customer who does not meet these conditions remains a customer of ECNG Digital Sp. z o.o. A refusal, lack of agreement, failed check or Cornerstore rejection does not create a relationship with Cornerstore. For eligible EU/EEA customers, additional documented conditions may apply.

The temporary transition period allows ECNG Digital customers to decide whether they wish to migrate to Cornerstore. During this period, ECNG Digital remains the controller for all customers until novation is fully completed. Cornerstore becomes the controller only after acceptance, onboarding, and confirmation of all regulatory checks.

3. What data do we use and where does it come from?

Depending on the service and your status, we may use the following data:

Type of data	Examples
Account and contact data	Name, email address, telephone number, address, country, account credentials and communications.

Type of data	Examples
Identity and business-verification data	Date and place of birth, ID details and copies, liveness/video checks, company documents, beneficial-owner information, proof of address and authority to act.
Financial and transaction data	Bank details, wallet addresses, balances, transactions, transfer details, originator and beneficiary information, payment and account history.
Compliance, risk and security data	AML/KYC/KYB/KYT records, source-of-funds information, sanctions/PEP/adverse-media results, risk assessments, blockchain analytics, device/IP data, alerts and audit logs.

Most data come from you or from your use of the service. We may also receive data from identity-verification providers, banks and payment partners, blockchain and transaction-monitoring providers, public sanctions/PEP lists, business registers and competent authorities.

Some data are required by law or are necessary to provide the service. Without required identity, compliance, account or transaction information, we may be unable to open, continue or transfer an account, or process a transaction.

Cornerstore also processes personal data to comply with Costa Rican AML/CTF obligations and other applicable law and regulations.

4. Why do we use your data?

Purpose	What this includes	Legal basis
Provide and administer the service	Create and operate accounts, process transactions, provide support, handle novation and communicate with you.	Contract performance - Article 6(1)(b) GDPR.
Meet AML, sanctions and Travel Rule duties	Verify identity, assess risk, monitor transactions, detect suspicious activity and make required reports or disclosures.	Legal obligation - Article 6(1)(c) GDPR. Where necessary, substantial public interest under Article 9(2)(g) and applicable AML law.
Keep legally required records	Meet retention, accounting, tax, audit, investigation and regulatory duties.	Legal obligation - Article 6(1)(c) GDPR.
Protect people, data and the platform	Prevent fraud, secure accounts and systems, investigate incidents and defend legal claims.	Legitimate interests - Article 6(1)(f) GDPR, and legal obligations where applicable.
Handle complaints and legal matters	Respond to requests, complaints, disputes, audits and claims.	Legitimate interests and/or legal obligation - Article 6(1)(f) and 6(1)(c) GDPR.
Marketing	Send information about our own services where allowed by law.	Consent where required, or legitimate interests for similar services where allowed. You can opt out at any time.

We do not intentionally collect special-category data unless it is strictly necessary for a legal requirement. Where facial image or video is used for identity verification, we process it only as permitted by applicable law and only where necessary.

5. Cornerstore storage, retention and international access

All retained Cornerstore data stays on EU/EEA servers

Cornerstore will store and retain all personal data transferred to it under this temporary arrangement - including live records, backups, archives and disaster-recovery copies - only on servers located in the EU or EEA. Cornerstore will not store, replicate or retain that transferred data on servers outside the EU/EEA.

Cornerstore applies all contractual, technical, and organizational safeguards required by applicable law for cross-border personal data transfers.

Cornerstore will protect this data with measures appropriate to the risk, including least-privilege access, role-based permissions, multi-factor authentication where appropriate, encryption and secure transmission where appropriate, logging, monitoring, access reviews, incident-management procedures, secure backups and regular security testing.

Storage in the EU/EEA does not by itself remove the GDPR rules on international transfers. If an authorised Cornerstore person or service provider accesses the data from Costa Rica or another country outside the EU/EEA, that access will be treated as a restricted transfer. It will happen only where a valid GDPR transfer mechanism and appropriate safeguards are in place, such as the European Commission Standard Contractual Clauses, a transfer assessment and additional technical or organisational safeguards where needed.

Cornerstore and ECNG Digital Sp. z o.o. must keep written data-transfer arrangements that identify their roles, the data used, the purpose, recipients, sub-processors, security measures, retention, breach handling, data-subject requests and the required end-of-term return or deletion process.

6. Who may receive your data?

We share data only where necessary and lawful. Recipients may include:

- the controller responsible for your customer status and, for a valid novation, Cornerstore;
- ECNG Group companies and approved processors providing technology, hosting, security, support, verification, blockchain-monitoring, analytics or professional services;
- banks, payment partners, other crypto-asset service providers and Travel Rule participants where information must accompany a transaction;
- auditors, insurers, lawyers and advisers; and
- competent authorities, regulators, law-enforcement bodies and courts where disclosure is legally required or necessary to protect rights or prevent fraud.

Processors may use personal data only on documented instructions and for the services they provide. They must be subject to contractual and security controls. For virtual asset transfers, Cornerstore may share originator and beneficiary information with other crypto/virtual-asset service providers and financial institutions where required by law (eg. FATF Recommendations)

7. How long do we keep data?

Retention is specific to each controller. A migration or novation does not end, restart or remove another controller's legal retention duty. When data are no longer needed, the relevant controller deletes, anonymises or securely archives them unless the law or a claim requires further retention.

Controller	Records	Retention rule
ECNG Digital UAB	Legacy records from the relationship handled by UAB before 22 December 2025.	8 years from the end of the business relationship or completion of the relevant transaction, as applicable, subject to a lawful extension, investigation, proceeding or claim.
ECNG Digital Sp. z o.o.	Records from before an individual novation, all Non-Novated Customers, and its own statutory, operational and historic records.	AML/CTF documentation and transaction evidence: generally 5 years from the end of the relationship or relevant transaction, subject to any lawful extension. Other data: the applicable statutory, limitation, security, complaint or claims period.
Cornerstore	Data transferred for a valid Novated Customer and data created by Cornerstore after novation.	For the period needed to provide the temporary service and for the legal, regulatory, accounting, audit, security, complaint and claims periods that apply to

Controller	Records	Retention rule
		Cornerstore. It will be stored and retained on EU/EEA servers throughout that period.

At the end of the temporary period, Cornerstore's platform access ends except as needed for a lawful wind-down, customer-asset protection, reconciliation, dispute handling and record preservation. Expiry does not automatically move a customer back to ECNG Digital Sp. z o.o. and does not require ECNG Digital UAB or ECNG Digital Sp. z o.o. to delete records they must keep.

8. Automated checks, security and data breaches

We use automated tools, such as transaction-risk scoring, sanctions screening and blockchain analytics, to identify fraud, suspicious activity and compliance risks. These tools support our teams. We do not make solely automated decisions with legal or similarly significant effects without meaningful human review.

Each controller is responsible for the security of its own systems and processing. If an incident affects the temporary service, ECNG Digital Sp. z o.o. and Cornerstore will cooperate to contain, investigate and remediate it. The controller responsible for the incident will meet its own GDPR breach-notification and communication duties.

9. Your privacy rights

Subject to legal limits, you may ask the relevant controller to:

- confirm whether it uses your data and give you access to it;
- correct inaccurate data;
- delete data where it no longer has a lawful reason to keep it;
- restrict or object to certain processing;
- provide data you gave us in a portable format, where the GDPR applies;
- withdraw consent at any time where we rely on consent;
- receive information about international-transfer safeguards; and
- request human intervention and contest a significant automated decision, where Article 22 GDPR applies.

For ECNG Digital Sp. z o.o. and ECNG Digital UAB, email dpo@ecng.digital. For Cornerstore's own post-novation processing, email info@mycorner.digital. We may ask for information to verify your identity. We normally respond within one month; the GDPR allows more time for complex or numerous requests, in which case we will tell you.

A deletion request may be limited where a controller must keep data for AML/CTF, tax, accounting, audit, regulatory, security or legal-claim purposes.

You may complain to the data-protection authority in your usual residence, workplace or place of the alleged breach. For ECNG Digital Sp. z o.o. this may include the Polish authority (UODO); for ECNG Digital UAB legacy processing, the Lithuanian authority may also be relevant.

10. Marketing, cookies, minors and changes

Marketing

Service, security, legal and transition messages are not marketing. We send them when needed to administer or protect an account, explain customer status, or communicate a restriction or wind-down. Marketing is sent only where permitted by law. You can opt out at any time using the unsubscribe option, your account settings where available, or the contact details above.

The transition must not be used to pressure or market to EU/EEA customers to obtain Cornerstore services or sign any reverse-solicitation declaration. Only factual, non-promotional notices about options, rights, restrictions or wind-down may be sent.

Cookies

We use necessary cookies to operate and secure ecng.digital. Analytics, preference and other non-essential cookies are used only where required consent has been obtained. Further information is in the Cookie Policy at https://files.ecng.digital/cdn/policy/cookie.

Minors

The services are not intended for people under 18 or below the legal age to form a binding contract under applicable law.

Changes

We may update this policy when legal, technical or operational circumstances change. A material update will be notified where required. This temporary notice must be reviewed before the end of the temporary transition.

11. Contact us

ECNG Digital Sp. z o.o. and ECNG Digital UAB privacy contact: dpo@ecng.digital.

Cornerstore Digital Limitada privacy contact for post-novation processing: info@mycorner.digital.

Last revised: 1 July 2026.