

Privacy Policy – C.O EL NIGERIANO J.J

Effective date: Immediate

Last revised: September 23, 2025

Controller/Owner: C.O EL NIGERIANO J.J (“Company,” “BRAND”)

Site: <https://coelnigerianojj.com>

Privacy contact: sales@coelnigerianojj.com • P.O. Box 20741, San Juan, PR 00928

1. Statement of principles, scope, and basis
 - 1.1 Commitment and standard. We process personal data under the principles of lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and proactive accountability. This standard derives from consumer-protection and privacy rules applicable in Puerto Rico/U.S. and from international best practices (privacy by design & by default).
 - 1.2 Material scope and channels. This Policy governs the Site, subdomains, checkout flows, post-sale, helpdesk, integrations with payment gateways and logistics, and any form or interface enabled by the Company.
 - 1.3 Not a substitute for T&Cs. This Policy forms part of the Terms & Conditions (T&Cs). In case of an interpretative conflict, the most protective rule for the User will prevail without distorting contractual obligations.
 - 1.4 Who’s who (functional summary).
 - a) Controller: Company.
 - b) Processors: contracted providers (hosting/CDN, payment gateway, logistics, anti-fraud, helpdesk).
 - c) Independent third parties: services with their own policies when you interact with them voluntarily (e.g., social networks).
2. Legal bases for processing (rationale)
 - 2.1 Contract performance: essential to create an account, process orders, invoice, ship, handle RMAs and warranties. Without this data, the sale is not viable.
 - 2.2 Compliance with legal obligations: tax/accounting, product safety, handling of claims, chargeback management, and cooperation with competent authorities.
 - 2.3 Legitimate interest (balanced and documented): security (WAF/anti-bot, logs), fraud prevention (risk signals, reasonable verification), service improvement and operational metrics (without invasive profiling), business continuity.
 - 2.4 Consent: non-essential cookies/SDKs, newsletters, and electronic marketing; you may withdraw consent at any time (no retroactive effect).
 - 2.5 Vital interest/public order: only in exceptional cases (e.g., user safety, product health alerts).
3. Data categories and purposes (exhaustive map)
 - 3.1 Identification and contact (name, email, phone, addresses): registration, support, shipping, billing.
 - 3.2 Transactional (cart/orders, amounts, products, gateway tokens/IDs; never full PAN or CVV): charges, refunds, reconciliation, anti-fraud.
 - 3.3 Technical/security (logs): IP, user-agent, reasonable device ID, timestamps, authentication attempts, MFA, sensitive changes, WAF/anti-bot/API events:

cybersecurity, continuity, compliance.

3.4 Support/post-sale: photos/videos for claims, RMA, communications: verification of incidents and warranties.

3.5 Preferences/marketing: opt-in/opt-out, cookie settings; sending lawful communications and aggregated measurement.

3.6 KYC/Verification (B2B/high risk): entity/representative data, good standing, exemption/reseller certificates: risk management, legitimizing the relationship.

3.7 We do not request sensitive categories (health, biometrics, etc.). If the User submits them by mistake, they will be deleted or shielded with enhanced measures.

4. Data sources and relevance criteria

4.1 Direct (provided by the User); automatic (technical interaction with the Site); derived (gateways/carriers: confirmations, tracking).

4.2 Relevance: we only request what is strictly necessary for the stated purpose. Forms use minimum fields and basic validations (e.g., verified email).

5. Cookies/SDKs and consent management platform (CMP)

5.1 Categories: strictly necessary (active by default), functional, analytics/measurement, advertising.

5.2 Activation regime: non-essential categories only load with opt-in. We record a consent log (version, date/time, preference).

5.3 Management: you can revoke or adjust preferences at any time from the panel. Technical details appear in the Cookie Notice (an integral part of this Policy).

5.4 Do Not Track: we do not currently respond to browser DNT signals if the standard is not uniform; we honor CMP consent.

6. Payments: security and no storage of credentials

6.1 We process payments exclusively through PCI DSS providers (e.g., Stripe/PayPal/ATH Móvil Business, as disclosed at checkout).

6.2 The Company does not store PAN/CVV. We retain non-sensitive tokens for reconciliation, refunds, and anti-fraud management.

7. Processors/third parties: contracts and safeguards

7.1 Every processor signs a contract covering confidentiality, equivalent security, purpose limitation, sub-processor controls, and early incident notification.

7.2 In optional integrations (e.g., social networks, maps), your data is also governed by those third parties' policies. We recommend reviewing them before use.

8. International transfers

8.1 We only make transfers necessary for operations (e.g., global CDN, gateway, cloud). Where they involve countries without an "adequate" level, we apply Standard Contractual Clauses or equivalent safeguards and a destination risk assessment.

8.2 We do not transfer data to sanctioned jurisdictions nor in contravention of export controls.

9. Retention and deletion

9.1 General rule: "only what's necessary, for as long as necessary."

- Account and profile: active relationship + up to 2 years (defense against claims).
- Billing/accounting: 5–7 years (tax requirements).
- Security logs: authentication 12 months; critical events 24 months; incidents: until closure + legal time limits.
- Marketing: while consent or relationship remains, or until opt-out.

9.2 We implement secure deletion or anonymization upon expiry, with a record of the action.

10. Security (defense in depth)

10.1 Technical/organizational controls: TLS; encryption in transit and, where applicable, at rest; MFA on sensitive access; least privilege; WAF/IDS/IPS; rate-limiting/anti-bot; environment segregation; backups; patch management; monitoring; vulnerability testing and, where appropriate, pentesting.

10.2 Key management: periodic rotation, secure vaults, prohibition on secrets embedded in code.

10.3 Evidentiary integrity: for high-impact incidents, an evidence package with timestamping, hashing, and chain of custody.

11. Anti-fraud and reasonable verification (KYC)

11.1 We may require verification (email/phone, address, cardholder-payment match, identity or corporate documents) when risk signals arise: multiple failed attempts, identity/address discrepancies, risky IP/TOR/ASN, unusual coupon use, chargeback history.

11.2 Principles: non-discrimination, minimization, and processing consistent with this Policy.

11.3 Proportionate measures: request for additional information, temporary order hold, cancellation with refund, account closure, blocking of irregular payment methods/devices.

12. User/Customer rights and request handling

12.1 Rights: access, rectification, update, deletion, objection, restriction, and portability (where applicable).

12.2 How to exercise: sales@coelnigerianojj.com or the Site form. Acknowledgment ≤ 5 business days; resolution ≤ 30 days (extendable for complexity with notice).

12.3 Proportionate identity verification to protect accounts/data (e.g., confirmation via verified email). Anti-retaliation: no adverse treatment for exercising rights.

12.4 Marketing: immediate opt-out via the unsubscribe link or preferences panel; SMS is governed by the TCPA (express written consent; text “STOP” to unsubscribe).

12.5 Appeal/Review (when required by applicable state law): you may request a review of a negative response; we will indicate channel and timeframe.

13. Minors

13.1 We do not target the Site to children under 13 nor knowingly collect their data without meeting legal requirements (e.g., verifiable parental consent).

13.2 To contract: ≥ 18 years old or verifiable consent of a legal representative (who assumes the obligations of the transaction).

14. Security incidents and notifications

14.1 We activate the Incident Response Plan (IRP): detection → containment → analysis → remediation → notification (as applicable) → post-mortem.

14.2 Where required by law, we will notify authorities and/or affected individuals with: description of facts, scope, risks, measures adopted, and recommendations (including credential rotation).

14.3 Evidence preservation: logs, snapshots, and hashes for the time strictly necessary to investigate and document actions.

15. UGC, intellectual property, and DMCA

15.1 User-Generated Content (UGC) may be used under the license set out in the T&Cs (hosting, reproduction, public communication on official channels).

15.2 We handle DMCA notices (notice & takedown); notice requirements and the designated agent appear in the T&Cs.

16. Contractual bases and proof of acceptance

16.1 Acceptance of this Policy and the T&Cs is validly formalized by electronic means (E-SIGN Act, UETA where applicable, Puerto Rico Electronic Signatures Act).

16.2 We keep evidence: date/time, IP/user-agent, text version, and hash of the accepted version.

17. Changes to this Policy

17.1 We may modify/update the Policy for legal, technical, or operational reasons. The in-force version will be the one posted on the Site with its date.

17.2 Where appropriate, we will send a general notice to registered users. Continued use implies awareness of the current version without prejudice to mandatory rights.

ANNEX I — Retention Table (guidance)

- Account/Profile: term + up to 2 years.
- Billing/accounting: 5–7 years.
- Authentication logs: 12 months; critical events: 24 months; incidents: until closure + legal period.
- RMA/Claims: until closure + applicable statute of limitations.
- Marketing: while consent/relationship remains or until opt-out.

ANNEX II — Security framework (operational summary)

- Controls: TLS, encryption in transit/at rest (where applicable), MFA, least privilege, WAF/IDS/IPS, rate-limiting/anti-bot, prod/test segregation, backups, patch management, vulnerability scans, pentest where applicable.
- Secret management: vaults, rotation, no embedded secrets.
- Logs: authentication (success/failure), MFA, sensitive changes, payments (transaction ID, not PAN/CVV), signed webhooks, cookie decisions, T&C acceptance (hash).
- Evidentiary integrity: time-stamping and hashing of evidence packages.

ANNEX III — Sector notices and compatibilities

- HIPAA: we are not a “covered entity” nor a “business associate”; unless otherwise agreed/specific activity, HIPAA does not apply.

- CAN-SPAM/TCPA: email/SMS marketing requires a valid legal basis; SMS requires express written consent; “STOP” to unsubscribe.
- Advertising: we comply with FTC Endorsement Guides/Green Guides where applicable; disclosure of material relationships with endorsers; reasonable substantiation of claims; consistency with your T&Cs (responsible advertising).
- Export controls/OFAC: we do not operate with sanctioned jurisdictions/persons.

ANNEX IV — Jurisdictional Rights Notice (U.S. + EU/UK)

A) California consumers (CPRA) and states with analogous laws (VA/CO/CT/UT, etc.)

A.1 CPRA categories we may process (as applicable): identifiers (A), customer records (B), commercial information (D), internet/network activity (F), limited inferences (H) without invasive profiling; we do not process sensitive categories except for minimal, informed verification.

A.2 Purposes: see Section 3. Retention: see Annex I. Sources: direct, automatic, gateways/carriers.

A.3 Disclosures to third parties: only to processors for operational purposes; we do not sell personal data nor engage in “sharing” for cross-context behavioral advertising without your prior opt-in (where applicable) and opt-out always available.

A.4 Rights: know/access, correction, deletion, opt-out of sale/sharing (if ever applicable), non-discrimination. GPC (Global Privacy Control) signal: we honor it for CPRA-subject flows when it can be verifiably linked. Appeal: a review channel is available in case of denial (details provided in our response).

A.5 Minors: we do not sell/share data of minors under 16.

B) European Economic Area/United Kingdom (GDPR/UK GDPR)

B.1 Controller: Company (details in the header). DPO/Privacy Lead: appointed internally; contact via sales@coelnigerianojj.com.

B.2 Bases: Art. 6(1)(a), (b), (c), (f) as applicable (see Section 2). Legitimate interest documented with a balancing test.

B.3 Transfers: where applicable, SCCs/UK IDTA or another valid instrument + a destination risk assessment.

B.4 Rights: access, rectification, erasure, restriction, objection, portability, and not to be subject to decisions based solely on automated processing with legal or similar significant effects (we do not carry out such decisions). Complaint: competent supervisory authority; we invite you to contact us first.

B.5 Retention/Security: see Annexes I–II.

Highlighted understanding clause (executive summary for the user)

- We do not sell your data or engage in “sharing” for behavioral advertising without your legal basis/opt-in where required; opt-out is always available.
- We operate with PCI DSS gateways; we do not store PAN/CVV.
- You can access/correct/delete/restrict/object/port (where applicable) and unsubscribe from marketing at any time.
- We maintain an incident plan, logs, and controls to protect your data.
- Non-essential cookies only with your consent via the CMP.

