

EU Reverse Solicitation Policy & Procedure

Version 1.0 | Internal Policy and Operating Procedure

Document Control	Details
Legal entity	Novara S.A. de C.V. (verify legal name and registration details before adoption)
Document ID / Version	NVR-COM-001 / 1.0
Date / Status	09 October 2026 / FINAL DRAFT – pending formal approval
Document owner	Compliance function
Approval	Management / competent governing body – pending
Next review	No later than 12 months after approval or sooner following a relevant change
Linked form	NVR-COM-002 – EU Reverse Solicitation Compliance Checklist v1.0

Approval condition: This document is an implementation-ready draft. It becomes binding only after verification of the legal entity, licensing status, products, data-protection framework and jurisdiction matrix, and formal approval. Approval of an individual case under this Policy does not replace any authorisation required under other laws.

1. Purpose and Governing Principle

This Policy establishes eligibility conditions, exclusions, responsibilities, controls, approval steps and evidentiary requirements for the exceptional case in which a customer established or resident in the European Union (EU) requests a specific crypto-asset service from Novara entirely at the customer's own exclusive initiative. Its legal basis is Article 61 of Regulation (EU) 2023/1114 (MiCA), interpreted in light of ESMA Guidelines ESMA35-1872330276-2030.

Binding principle: The EU is not a routinely supported sales or onboarding market. Neither Novara nor persons acting on its behalf may actively or indirectly solicit EU customers for the services concerned. Reverse solicitation is not a distribution strategy, a customer-acquisition programme or a substitute for MiCA authorisation.

A customer declaration, disclaimer, checkbox, general website accessibility or a small number of cases does not in itself establish an exception. The actual, documented circumstances of each contact are decisive.

2. Scope and Limitations

This Policy applies to Novara, its employees and management, contracted service providers, affiliates, sales and referral arrangements and technical channels insofar as they influence EU-related contacts or services. It covers natural and

legal persons resident or established in the EU or otherwise located in the EU where that is legally relevant. Citizenship, IP address or self-declaration alone is not determinative; inconsistencies must be resolved.

For non-EU EEA countries (Iceland, Liechtenstein and Norway), the United Kingdom, Switzerland and other countries, applicable local law must be assessed separately. This Policy does not assume that Article 61 MiCA automatically extends territorially to every EEA or third-country case. Novara may apply equally strict internal restrictions to those jurisdictions as a precaution.

Article 61 MiCA addresses only the MiCA authorisation requirement for crypto-asset services within its scope. Payment services, e-money, accounts/IBANs, cards, lending, securities/financial instruments, consumer protection, AML, sanctions, data protection and national requirements must be assessed independently. This Policy does not authorise Columis/card/payment functionality.

Before any assessment, confirm that the contracting entity is genuinely a third-country undertaking established outside the EU, that the specific service falls within MiCA, and that provision is permissible under its home-country law and other applicable national law. No assumption of EU rights or authorisation may be inferred solely from any regulatory status in El Salvador.

3. Legal and Interpretative Principles

Article 61(1) MiCA: A specific crypto-asset service provided at the customer's own exclusive initiative may fall outside the Article 59 MiCA authorisation requirement; direct or indirect solicitation by the firm, related persons or persons acting on its behalf defeats this rationale.

Article 61(2) MiCA: The initial initiative does not authorise marketing of new types of crypto-assets or crypto-asset services. ESMA also takes a restrictive approach to subsequent marketing of services of the same type outside the context of the original transaction.

ESMA Guidelines 1–2: Solicitation can involve advertising, websites, SEO, pop-ups, social media, sponsorships, affiliates, influencers, referrals and redirections. Remuneration is strong evidence, but not an indispensable condition, of acting on behalf of the firm.

ESMA Guidelines 3–4: Proof of customer initiative requires a fact-specific assessment. The concept of the “same type” is construed narrowly, considering the service, crypto-asset category, technology and risks.

4. Definitions

Term	Internal working definition
EU-RS case	An individual case potentially falling within Article 61 MiCA, assessed before any service is provided.
Own exclusive initiative	An unsolicited, independent customer request for a specific service without attributable solicitation by Novara or third parties.
Initial request	Earliest verifiable customer-initiated communication specifying a service; a website visit alone is insufficient.
Solicitation	Direct or indirect advertising, promotion, invitation, outreach or other customer acquisition by Novara or attributable third parties.

NOVARA S.A. de C.V.

Avenida Revolucion 25, Floor 6
Presidente Plaza, San Salvador, El Salvador
info@columis.com



Term	Internal working definition
Service scope	Documented, narrowly defined service/transaction, crypto-assets and technical permissions.
Hard stop	A prohibition or irremediable inconsistency; no approval through the RS process.
Hold / escalation	Incomplete or inconsistent information; no approval until satisfactorily resolved.

5. Roles and Responsibilities

Function	Responsibility / control principle
Management	Approves the Policy, risk appetite and exceptions to internal controls (not applicable law); receives regular reports and escalated cases.
Compliance Officer	Owns the RS process; issues independent, documented case decisions; monitors acquisition channels, service scope, controls and reviews.
Legal / external EU counsel	Reviews borderline cases, legal changes, national requirements and mixed crypto/payment/card offerings; does not provide blanket or fictitious approvals.
KYC/AML/Sanctions	Separately reviews identity, beneficial owners, PEP status, sanctions, AML risk and other mandatory onboarding requirements.
Marketing / Partnerships	Prevents EU targeting and indirect solicitation; documents campaigns, affiliates, referrals and sponsorships.
Product / Engineering	Enforces the EU block in the standard flow, role-based approvals, entitlements, marketing suppression and tamper-evident logs.
Customer Support / Sales	Handles only unsolicited factual enquiries; no active expansion of offers or sales follow-up; escalates EU connections.
Data protection function	Reviews data minimisation, legal basis, notices, access and retention rules.

Segregation of duties: Sales, Support and affiliates may neither approve an EU-RS case independently nor activate entitlements. A conflicted Compliance Officer must not decide the case; an alternate approver or second approval must be designated.

6. Mandatory Eligibility Conditions

- An unsolicited, verifiable initial customer request preceding any attributable outreach or solicitation to that customer.
- A specific description of the requested crypto-asset service and, where relevant, the crypto-asset, transaction or intended scope.
- No substantiated evidence of EU-directed solicitation attributable to Novara, affiliates, staff, agents or other persons acting in fact on its behalf.
- A plausible and verified source of contact supported by preserved primary evidence; a customer declaration supplements but does not replace factual verification.
- A favourable legal assessment of third-country status, product classification, EU/national law, home-country law and any other applicable regimes.
- Separate AML/KYC/sanctions clearance as required before activation, and written Compliance approval defining precise service entitlements.

7. Exclusion Grounds and Risk Indicators

7.1 Hard Stops – Normally Reject

- Prior direct outreach by Novara or an attributable third party intended to win the customer for the service; a documented EU-targeted campaign in the relevant market or channel.
- Customer acquisition through paid EU affiliates, influencers, sales agents, referral/lead programmes, or targeted redirection by an EU group company or EU-regulated provider.
- False or manifestly misleading declarations, manipulated acquisition evidence, deliberate circumvention of geoblocking or material inconsistencies that cannot be credibly resolved.
- A service that cannot lawfully be approved, unresolved or adverse legal conclusions under MiCA, home-country or other applicable law, or applicable sanctions/AML disqualification.
- Proposed bundled product packages, automatic activation of unrelated services or cross-selling beyond the customer's own request.

7.2 Hold / Enhanced Review – Not Automatic Rejection

- Organic search, broad brand advertising, media coverage, independent reviews, social-media mentions or personal recommendations: the source alone proves neither compliance nor non-compliance. Attribution, reach and actual circumstances must be assessed.
 - EU IP address, EU language, EU telephone number, temporary travel location or foreign nationality are indicators only; assess residence, establishment and actual circumstances.
 - Incomplete referral or campaign records, unexplained UTM parameters, third-party contacts, inconsistent timestamps or unclear service classification.
- Where material uncertainty cannot be resolved, do not approve. There is no permissible numerical threshold or safe harbour for the number of EU-RS customers.

8. Procedure and Decision Gates

Gate	Mandatory step	Outcome
G0 – Default block	Detect EU connections in registration/KYC; block standard activation; no RS promotion or self-unlock checkbox.	Blocked / case opened

Gate	Mandatory step	Outcome
G1 – Intake	Record only a genuinely unsolicited inbound request; preserve initial contact, channel, original content and UTC timestamp.	Case ID / evidence
G2 – Origin	Check marketing, referrals, affiliates, CRM, campaigns and group contacts retrospectively; obtain customer’s own account of origin.	Pass / Hold / Reject
G3 – Legal and scope	Document third-country status, MiCA service, asset type, territorial/national limits, home-country law and other regimes.	Pass / Legal Hold / Reject
G4 – Controls	Review factual customer declaration, KYC/AML/sanctions, product clearance, privacy and technical restrictions.	Pass / Hold / Reject
G5 – Approval	Compliance signs a reasoned decision; Legal review when escalation is mandatory; four-eyes approval for defined high-risk cases.	Approved / Rejected
G6 – Activation	Activate approved scope only; disable marketing/referrals/promotional pushes; archive versioned evidence.	EU-RS restricted
G7 – Ongoing review	Review new customer-initiated requests, changes, complaints, marketing matches and red flags; suspend promptly if required.	Continue / Suspend / Exit

Approval is valid only when the case file is complete, all mandatory controls have passed, the decision is dated before activation, and technical restrictions have been demonstrably applied. Management may not override statutory exclusions.

9. Evidence and Customer Declaration

Each case must include at least: case ID, customer identifier, residence/place of establishment, original initial communication, original UTC timestamps, channel, customer’s own description of how they found Novara, URL/UTM/referrer where available, referral/affiliate checks, documented marketing/CRM checks, applicable jurisdiction/product assessment, specific service request, factual customer declaration, Compliance decision, approver, technical entitlements and subsequent events.

Customer declarations must not force a pre-written legal conclusion disguised as an admission of fact. Appropriate questions are factual (e.g., “How did you first hear about Novara?” and “Which service did you request yourself?”). Declarations must be truthful and voluntary and must never be used to override proven solicitation.

Evidence handling: preserve original evidence without alteration and record its source; version subsequent changes; limit access on a need-to-know basis; use consistent UTC timestamps and timezone information; use screenshots only as supplements to source records. Do not collect personal data covertly or beyond what is necessary for the purpose.

10. Service Scope, Communications and Technical Controls

Apply an EU-RS account/product flag and maintain granular entitlements for each service, crypto-asset category and, where relevant, transaction; never grant automatic “all products” access.

Factual transaction-related communications and necessary service/security notices may continue; suppress promotional messages, retargeting, newsletters, trading pushes, cross-selling, referral incentives and sales calls. A later customer request for another product, service or new transaction context requires a new documented customer initiative and renewed scope assessment. Distinguish ongoing contractual obligations within the specifically requested original service.

Do not automatically equate “same type” with the same blockchain, currency or product menu. Assess risk, asset category, technology and timing.

Card, IBAN, payment and other services not clearly covered by MiCA must remain disabled until separately cleared by Legal.

Test controls before go-live and following releases: country gate, manual approval, role permissions, entitlement matrix, marketing suppression, tamper-evident audit trail and suspension/revocation mechanisms.

11. Monitoring, Incidents and Escalation

Compliance maintains a central EU-RS register of approvals, rejections, pending cases, services, acquisition sources and relevant events. At least quarterly, sample case files and test the effectiveness of marketing suppression; regularly reconcile marketing/partner lists and campaign parameters. Increase scope and frequency based on risk.

Immediately escalate to Compliance and Legal suspected EU targeting, prohibited third-party acquisition, misleading declarations, unintended service activation, regulatory requests, customer complaints or material legal changes. Compliance may immediately suspend activation and marketing, require reassessment, reject the case or initiate a legally reviewed exit.

Handle regulatory information requests and complaints in a traceable and timely manner, respecting confidentiality, data protection and applicable reporting obligations. Record root cause, remediation, owners and final verification.

12. Retention, Data Protection and Change Management

Retention periods, deletion and preservation requirements must be set out in a separate, legally reviewed retention schedule; this Policy does not assert a universal statutory retention period. Consider applicable AML, contractual, tax, supervisory and data-protection duties, limitation periods and legal holds. Minimise and adequately protect personal data.

Before implementing changes to websites, SEO, languages, domains, referral/affiliate arrangements, marketing channels, product catalogue, group cooperation or geofencing, Compliance must assess EU-solicitation risk. Material changes trigger a Policy review.

13. Decision and Documentation Standard

The written case decision must record at least: (i) specific facts and sources; (ii) assessment of exclusive customer initiative and potential attribution; (iii) relevant jurisdiction and MiCA/other-law assessment; (iv) precise service scope; (v) outstanding risks and mitigations; and (vi) approver, date, conditions and review trigger. “Checkbox ticked” or “customer clicked independently” is not sufficient reasoning.

Decision categories: APPROVE (complete evidence, lawful scope, effective controls); HOLD (evidence or legal review outstanding, no activation); REJECT (exclusion, unresolved material doubt or unlawful service); SUSPEND/REVOKE (requirements subsequently cease to be met). Record every decision in form NVR-COM-002.

14. Effective Date and Formal Approval

Required clearance before operational use	Evidence / status
Legal entity, registered office and home-country permissions verified	_____
EU/national legal assessment of offered products	_____
Separate card/payment/e-money review, where relevant	_____
Data protection / retention schedule approved	_____
Technical blocks and control tests signed off	_____
Management: name / signature / date	_____

15. Legal Sources and References

[1] Regulation (EU) 2023/1114 (MiCA), particularly Articles 59 and 61, official EU legislation: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj>

[2] ESMA, Guidelines on reverse solicitation under MiCA, ESMA35-1872330276-2030, 26 February 2025, particularly Guidelines 1–4 and the Annex: <https://www.esma.europa.eu/document/guidelines-reverse-solicitation-under-mica>

[3] ESMA, Final Report on the Guidelines on reverse solicitation under MiCA, ESMA35-1872330276-1899, 17 December 2024: <https://www.esma.europa.eu/document/final-report-guidelines-reverse-solicitation-under-markets-crypto-assets-regulation-mica>

16. Annex – Practical Approval Matrix

Illustrative scenario	Standard treatment
Customer independently emails a specific BTC custody request without prior outreach; origin is plausible and verified.	Individual assessment possible; never automatic approval.
Customer comes from EU-targeted advertising, paid referral or EU group-company redirection.	REJECT; customer declaration cannot cure solicitation.
Customer finds Novara through general search or an independent third-party review.	HOLD pending assessment of SEO, campaigns, attribution and other circumstances; no safe harbour.
An approved customer receives a BTC-buy promotion or card advertising one month later.	Investigate unlawful expansion / marketing incident; stop the promotion and escalate.

NOVARA S.A. de C.V.

Avenida Revolucion 25, Floor 6
Presidente Plaza, San Salvador, El Salvador
info@columis.com



Illustrative scenario	Standard treatment
Customer later independently requests another service or asset type.	Capture new request and complete a separate documented scope/legal assessment before enabling.

Control note: Under the ESMA Guidelines, even broadly distributed brand advertising or promotions not exclusively targeting the EU may constitute solicitation in the EU. Evidence that a particular customer personally saw the advertisement is not always required for a relevant solicitation risk. The decision must assess the overall acquisition practices.