EU RegCORE Client Alert

Financial Services

June 2026

After the MiCAR Deadline: Enforcement, Liability and Legal Consequences for Non-Compliant CASPs from 1 July 2026

QuickTake

On 17 April 2026, the European Securities and Markets Authority (**ESMA**) issued a statement (reference ESMA75-113276571-1679)[1] clarifying supervisory expectations regarding the end of the transitional period under the Markets in Crypto-Assets Regulation (**MiCAR**). The statement forms part of a series of ESMA communications on this topic, following earlier statements on supervisory convergence (October 2023), transitional measures (December 2024) and the end of transitional periods (December 2025). The central message is unambiguous: the **MiCAR transitional period will officially expire across the EU on 1 July 2026** and after that date **any entity providing crypto-asset services to EU clients without a MiCAR licence will be in breach of EU law and must cease offering such services**.

The expiry of all MiCAR transitional arrangements on 1 July 2026 is not merely a licensing deadline — it is a fundamental legal transformation of the EU crypto-

Dr. Michael Huertas
Tel: +49 160 97375760
michael.huertas@pwc.com

Dr. Hagen Weiss
+49 1511 5708446
hagen.weiss@pwc.com

EU RegCORE Team
de_regcore@pwc.com

[1] Available here.

asset market. The legal implications extend well beyond licensing. The expiry fundamentally alters: the legality of existing business models; contractual relationships with clients; exposure of boards and senior management; supervisory expectations; enforcement risk; civil litigation exposure; and insolvency outcomes as applicable to crypto-asset services providers (**CASP**s). This Client Alert analyses the ESMA Statement's key themes and implications arising for regulated and unregulated CASPs, as well as practical considerations for clients and investors. The key elements are as follows:

- **What.** ESMA has issued a statement clarifying supervisory expectations as the MiCAR transitional period draws to a close on 1 July 2026. The statement sets out expectations for unauthorised CASPs regarding wind-down plans, expectations for authorised CASPs regarding client migration, expectations for national competent authorities (**NCAs**) regarding enforcement (and they have indicated they will enforce) and a warning for consumers to verify their provider's authorisation status. Entities established outside the EU are reminded that they are not permitted to provide crypto-asset services to EU investors outside the narrow exception of reverse solicitation.
- **When.** The MiCAR transitional period will officially expire across the EU on 1 July 2026. After this date, any entity providing crypto-asset services to EU clients without a MiCAR licence will be in breach of EU law and must cease offering such services. This applies irrespective of whether MiCAR has been implemented in a Member State or not. Entities that did not provide crypto-asset services in accordance with applicable national law before 30 December 2024 could never rely on the transitional regime. Entities in Member States with shorter transitional windows — notably Germany and Ireland (12 months) — were required to be authorised before the relevant deadline; for Germany, the effective deadline was end of December 2025.
- **Who.** ESMA's statement is addressed to: (i) **unauthorised CASPs** that must implement orderly wind-down plans and cease regulated services by 1 July 2026; (ii) **authorised CASPs** that must actively manage the migration of existing clients ahead of the deadline and ensure full compliance with applicable AML/CFT requirements; (iii) **NCAs** that are expected to verify wind-down plans, take enforcement action against unauthorised provision of services and scrutinise client migration strategies; and (iv) **consumers and investors** who should verify their provider's authorisation status in the ESMA Interim MiCAR Register[2] and act promptly if their provider is not authorised.

Key takeaways

The following sections set out the legal framework, supervisory expectations, liability exposure and practical steps that affected persons must address before, on and after 1 July 2026.

The Legal Position from 1 July 2026

The Cliff-Edge: No Extension, No Grace Period

The MiCAR transitional period expires uniformly across the EU on 1 July 2026. ESMA has stated explicitly that there will be no extension and that last-minute authorisation applications will not grant a grace period to continue operating past the deadline.

[2] Available here.

Two anterior carve-outs must already have been accounted for. First, entities that did not provide crypto-asset services in accordance with applicable national law before 30 December 2024 could never rely on the transitional regime. Second, entities in Member States that elected shorter transitional windows — notably Germany and Ireland (12 months) — were required to be authorised before 1 July 2026; for Germany, the effective deadline was end of December 2025.

A filed but undecided application provides no continued operating rights after 1 July 2026. Continued activity in that position is a breach of EU law, not a grey area.

The Regulated CASP Services

MiCAR Article 3(1) specifically defines categories of regulated crypto-asset service. Any person providing any of these to EU clients after 1 July 2026 without authorisation is in breach:

Service	MiCAR Article
Custody and administration of crypto-assets on behalf of clients	Art. 3(1)(17)
Operation of a trading platform for crypto-assets	Art. 3(1)(18)
Exchange of crypto-assets for funds	Art. 3(1)(19)
Exchange of crypto-assets for other crypto-assets	Art. 3(1)(20)
Execution of orders for crypto-assets on behalf of clients	Art. 3(1)(21)
Reception and transmission of orders on behalf of clients	Art. 3(1)(22)
Placing of crypto-assets	Art. 3(1)(23)
Transfer services, advice, and portfolio management	Art. 3(1)(24)–(26)

Non-custodial wallet providers — where the user retains sole control of private keys — are generally outside scope. However, smart contract wallets, multi-signature arrangements, and recovery mechanisms may not qualify depending on design and implementation. Classification errors are not a regulatory defence.

Consequences for Unauthorised Operators

Mandatory Cessation of Business

Firms without a MiCAR licence must stop providing regulated crypto-asset services to EU clients immediately on 1 July 2026. The obligation to cease is unconditional. ESMA and NCAs are expected to take enforcement action in cooperation with each other where service provision continues.

Regulatory Enforcement Toolkit

The enforcement toolkit available to NCAs includes: cease-and-desist orders and mandatory suspension of operations; public warnings and naming of non-compliant entities in the ESMA register; asset freezes and remediation orders; administrative financial penalties and recurring penalty payments under national implementing legislation; management bans — withdrawal of fit and proper status preventing executives

from holding positions at any EU regulated entity and referral for criminal prosecution — MiCAR does not displace national criminal frameworks applicable to AML, fraud, or market abuse, and exposure varies by jurisdiction.

France's AMF has explicitly warned of criminal penalties including up to two years' imprisonment and fines of €30,000 for post-deadline unauthorised operation alongside administrative blacklisting and court-ordered website blocking. Market consequences extend further: termination of banking relationships, payment rail restrictions, loss of counterparties and inability to obtain insurance.

Civil Liability Towards Clients of Unauthorised Operators

Clients of unauthorised operators are structurally advantaged in litigation. Multiple heads of claim are available:

- **Contractual invalidity.** Contracts entered into by an entity providing regulated services without authorisation are in several Member States either void or voidable at the client's election. Under French law, contractual nullity on grounds of *ordre public* may be invoked. German law treats contracts in breach of regulatory licensing requirements as potentially void under § 134 BGB (contracts *contra legem*). Given MiCAR's explicit consumer protection rationale, this analysis is likely to favour clients.

- **Regulatory tort.** An unauthorised CASP has no contractual defence because MiCAR's mandatory conduct standards apply as EU law. The client may bring claims combining breach of a duty imposed for the client's protection (*Schutzgesetz* under § 823(2) BGB in Germany), unjust enrichment and tortious misrepresentation.

- **Illegality-based claims.** Clients may argue: that contracts should not be enforced; that fees should be refunded; that profits made from unauthorised services should be disgorged and that operation without authorisation itself constitutes evidence of negligence in any claim for losses.

- **Reduced client protection.** ESMA has stated explicitly that clients remaining with unauthorised providers face limited legal protection and a greater risk of losing access to their assets — a direct factual foundation for civil claims.

Director and Senior Management Personal Exposure

Boards should not assume liability is limited to the legal entity. Personal exposure arises from: continuing operations without authorisation after 1 July 2026; inadequate wind-down planning or deliberate delay in triggering the wind-down plan while "trading through" after crossing prudential thresholds (wrongful trading); misleading client disclosures about authorisation status; failure to safeguard client assets during wind-down and insolvency-related misconduct including preferential treatment of selected clients.

Consequences include regulatory sanctions, management bans, civil claims and insolvency actions. Under Articles 68 and 74, executives carry fiduciary responsibility for ensuring an orderly exit. NCAs can issue multi-year professional bans preventing executives from holding management positions at any other EU financial or crypto institution.

Insolvency Risks

This area is frequently underestimated. Where a CASP fails financially, the key question is whether client assets are genuinely segregated. If segregation is ineffective: clients may become unsecured creditors

rather than asset owners; recovery values in insolvency may be substantially reduced; lengthy and expensive litigation follows regarding beneficial ownership, custody classification, tracing rights and insolvency estate claims; and preferential treatment of selected clients (for example, withdrawals prioritised for institutional clients or insiders over retail) constitutes illegal preferential treatment under Member State laws, triggering clawback mechanisms and personal director liability.

Having established the legal framework, the following section turns to what ESMA expects from market participants in practice — the operational requirements that NCAs may likely be expected to use to assess compliance.

ESMA's Supervisory Expectations: Wind-Down and Client Migration

Wind-Down Plans: Mandatory, Operational, and Immediately Executable

ESMA's April 2026 Statement establishes supervisory expectations — not recommendations — against which NCAs will assess firms. ESMA treats last-minute disorderly exits as a supervisory failure, not a standard business closure. Wind-down plans must be operational, credible, and immediately executable.

The plan must: enable an orderly exit without causing undue economic harm to clients; arrange transfer of client crypto-assets to an authorised CASP or to self-hosted wallets; provide clients with advance notice — not a same-day announcement — before triggering the plan; maintain all conduct, prudential, and AML/CFT obligations throughout the wind-down period; and be formally approved by the management body with a clear governance chain and a designated Wind-Down Officer as single point of contact for the NCA.

The AMF required DASPs to have plans operational and narrowed to strictly necessary wind-down activities by 30 March 2026 at the latest — with holders able to recover assets by transferring to an authorised CASP or selling with sufficient prior notice. Any firm that has not done so is already in a supervisory failure position.

Six Structural Components of an NCA-Compliant Wind-Down Plan

1. **Governance, Early Warning Indicators and Quantitative Triggers.** NCAs reject plans that lack objective activation criteria. The plan must specify: quantitative triggers — regulatory capital dropping below MiCAR prudential safeguards, irreversible net asset value depletion, catastrophic liquidity runs; qualitative triggers — final NCA licence refusal, loss of critical banking partner with no backup, uncurable custody hack or smart contract exploit and a decision matrix identifying which internal body (typically the Board) holds authority to activate the plan, with exact protocol for immediate NCA notification. The governance section must include a quantitative table of triggers; an NCA will not accept a wind-down plan that does not define exactly when activation occurs.

2. **Client Asset Migration Strategy — The Core Regulatory Focus.** This is the operational component that supervisors scrutinise most intensively. The plan must account for every client position. Two-pronged offboarding is required: individual withdrawal to self-hosted wallets or bulk migration to a pre-vetted partner CASP holding a valid MiCAR passport and actively listed on the ESMA Interim MiCAR Register. A "ghost account" protocol is needed: a legally segregated escrow structure for unresponsive users or unclaimed balances, with a clear legal framework for ongoing custody and ultimate disposition. For larger exchanges, tranche-based offboarding — phased by asset tier or geographic region — is required to avoid bottlenecking blockchain networks or overwhelming client support. The target partner CASP for bulk migration must be actively listed on the ESMA Interim MiCAR Register. If they are not,

the plan must rely strictly on individual self-hosted wallet withdrawals. Using an unauthorised third-country provider for sub-custody during wind-down is a direct breach.

3. **Financial Runway and Wind-Down Budget.** The firm must prove it has the capital to execute an orderly exit with zero incoming revenue. A dedicated standalone cash buffer — separate from daily operating capital — must cover: infrastructure and cloud hosting, legal fees, staff retention bonuses for critical teams and blockchain gas fees for clearing dust balances. Prudential capital safeguards must be maintained under MiCAR Article 67 right up until the final client asset is successfully offboarded.

4. **Operational Continuity and Critical Vendor Mapping.** The tech stack must remain live long enough for all users to exit. A critical vendor inventory is required covering: custody technology, KYC/AML screening, cloud infrastructure and liquidity providers. "Wind-down friendly" SLA provisions must prevent vendors from cutting off services the moment the plan is triggered.

5. **AML/CFT, Travel Rule, and Compliance Continuity.** Regulatory obligations do not end when trading stops. KYC, transaction monitoring, and Travel Rule protocols must remain fully active for all outbound asset transfers throughout the wind-down window. The wind-down process cannot be exploited as an exit channel for illicit capital.

6. **Post-Exit Data Archival and GDPR Compliance.** Two distinct obligations apply. First, secure storage of all trade logs and customer KYC records for the statutory 5-to-7-year EU AML data retention period in a locked cold-storage archive. Second, GDPR compliance on client data transfer: porting user data to a new corporate entity (the partner CASP) without a valid legal basis — explicit affirmative user consent or specific contractual necessity — violates GDPR and exposes the winding-down entity to statutory penalties of up to €20 million or 4% of global annual turnover. Mass consent failures during client migration represent a significant and frequently overlooked risk that can consume remaining wind-down reserves.

The Execution Timeline

ESMA expects a 30-to-90-day execution window from trigger to final licence cancellation:

Phase	Timeline	Key Actions
Trigger activation & NCA notification	Days 1–3	Board formally activates plan. Notification package submitted to home NCA. All marketing, affiliate links, and localised campaigns deactivated. New user registrations permanently locked.
Client notice & platform restriction	Days 4–14	Mandatory advance notice to all EU clients (email, push, UI banners). Fiat and crypto deposits disabled. New trading position creation halted. Withdrawal pathways kept fully optimised.
Position liquidation & active migration	Days 15–60	Core offboarding process. Users close open positions. Platform processes mass withdrawals to self-hosted wallets or initiates bulk transfer to authorised partner CASP. Support scaled for offboarding.

Final sweeps & decommissioning	Days 61–90+	Remaining assets moved to segregated escrow. Trading engine taken offline. API keys revoked. Compliance audit completed. Data archive locked. NCA formally cancels regulatory status.

Client Migration: Obligations on Authorised CASPs

Authorised CASPs face distinct obligations in onboarding migrating clients. Full, fresh AML/CFT customer due diligence must be conducted for every migrating client; inherited KYC files from an unauthorised predecessor will not survive NCA scrutiny. Suitability and appropriateness assessments must be completed for all new clients receiving advisory or portfolio management services — migrating clients cannot be "churned through" generic onboarding flows. NCAs scrutinise whether authorised CASPs are acting as fronts to enable unauthorised group entities to continue business-as-usual by funnelling transactions through the licensed entity. This constitutes piercing the corporate veil risk and joint-and-several liability for unauthorised group failures.

The wind-down and client migration framework applies to EU-established entities. For firms with third-country operations or group structures spanning multiple jurisdictions, additional constraints apply – these are set out below.

Third-Country Firms and the Reverse Solicitation Framework

The Third-Country Prohibition

Entities established outside the EU are not permitted to provide crypto-asset services qualifying as MiCAR services to EU investors, or to solicit EU clients for those services, unless the narrow reverse solicitation exception under Article 61 applies. This prohibition applies equally in a business-to-business context. Wind-down of EU operations does not resolve this: leaving offshore parent websites open to EU traffic while "winding down" EU entities is treated by NCAs as a major compliance breach.

Reverse Solicitation (Article 61): A Narrow Exception, Not a Business Model

The exemption allows a non-EU CASP to service an EU client only where that client requests the service on their "own exclusive initiative." Four rules determine the exemption's scope:

- **The "Own Exclusive Initiative" Rule.** The client must make the absolute first move entirely unsolicited. Boilerplate contractual disclaimers or "click-wrap" waivers — for example a checkbox stating "I confirm this transaction was executed at my own exclusive initiative" — do not override the physical facts of an interaction. If any prior marketing occurred, the exemption is void for that client and that transaction.

- **The Ultra-Broad Definition of Solicitation.** Solicitation is technology-neutral and covers any promotional activity reaching an EU audience, including: websites, mobile apps and push notifications; social media posts, SEO and use of financial influencers ("finfluencers"); sponsorships, brand advertising, roadshows and press releases; and even "purely educational" material is classified as solicitation if it contains links to a trading platform, provides onboarding paths, or distributes service brochures. EU-targeted country-code domains, localised language sites, geo-targeted advertising, EU app store presence and push notifications to EU users all constitute solicitation.

- **The "Person Soliciting" Test.** It does not matter who conducts the marketing. Activity by parent companies, offshore groups, affiliates or third parties with close links to the non-EU firm counts as solicitation regardless of whether payment is made. An EU-authorised entity cannot redirect its EU clients to an offshore affiliate: doing so is a direct MiCAR breach.

- **The "Same Type" Restriction.** A reverse solicitation request is strictly transaction- and product-specific. It does not open the door to ongoing relationship marketing or cross-selling. ESMA's granular asset taxonomy prevents firms from using a single client touchpoint to market an entire product suite:

Asset-Type Exclusions (Never "Same Type")	Service-Type Boundaries (No Cross-Selling)
MiCAR category mismatch: utility tokens, ARTs (asset-referenced tokens), and EMTs (e-money tokens) are entirely distinct categories	A request for investment advice does not authorise the cross-selling of custody services or portfolio management
Protocol/DLT variation: assets on separate, disconnected layer-1 or layer-2 networks	Packaged service suites cannot be offered when a client requested a single isolated execution transaction
Currency peg disconnect: if a client requests a EUR-pegged EMT, USD or GBP-pegged EMTs cannot be offered	The "Immediate Context Rule": same-type assets can only be displayed within the interface flow of the original transaction
Varying asset backing structures: fiat-backed ARTs are not the same type as algorithmic or crypto-collateralised ARTs	Any follow-on outreach by the firm after the initial transaction concludes requires a brand new, unsolicited client initiative
Divergent liquidity profiles: highly liquid assets are not the same type as illiquid or niche tokens	Once the initial client-initiated interaction concludes, the reverse solicitation window slams shut
Anonymity: tokens with no identifiable issuer are not the same type as tokens with a clearly identified corporate issuer	—

The Post-Wind-Down Reverse Solicitation Firewall

Firms that wind down their EU entities but leave offshore parent websites accessible to EU traffic remain exposed. The wind-down plan must include: hard geo-blocking of EU IP addresses on all platforms and interfaces; termination of localised marketing, EU app store presence and push notification access for EU users; absolute prohibition on onboarding previous EU users onto non-EU infrastructure during or after the wind-down window and contractual amendments to influencer and affiliate agreements prohibiting EU reach.

If a non-EU firm has not implemented strict geo-blocking, removed its app from EU app stores, updated influencer and affiliate contracts and disabled localised marketing, relying on reverse solicitation is a high-risk strategy that will likely fail NCA forensic audit.

NCA Forensic Audit Methodologies for Reverse Solicitation

Audit Technique	What NCAs Test
Mystery shopping & journey tests	Regulators simulate EU consumer journeys using local EU IP addresses, testing whether platforms actively block registration or prompt EU users to trade
Digital footprint sweeps	Automated tools scan for EU-specific indicators: country-code domains (.de, .fr, .lu), localised language options, geo-targeting cookies and regional SEO keywords
App store & push notification audits	NCAs verify whether the firm's app is available in EU-regional app stores and whether push notifications to EU-located users have been disabled
Data and record-keeping demands	NCAs require a "regulator-ready dossier": metadata logs proving the exact digital origin, timestamp, and context of the client's initial touchpoint
Whistleblower & cross-agency intelligence	NCAs collaborate with tax authorities and customs; tips from domestic competitor CASPs who lose market share to non-compliant offshore platforms are actively prioritised

Intragroup Structure Risk

MiCAR prohibits CASPs from outsourcing or delegating custody to entities not themselves authorised as CASPs. CASPs must ensure all outsourcing and delegation arrangements do not result in services being provided to EU clients via unauthorised third-country group entities. Two specific risks arise. First, the third-party custody restriction: an authorised CASP can only use another authorised CASP for sub-custody; using an unauthorised third-country custodian post-1 July is a direct breach, and the primary CASP remains 100% liable for any losses. Second, the intragroup fronting risk: if an authorised EU entity acts as a front for an unauthorised offshore affiliate — funnelling EU clients to the offshore entity via loopholes — the EU entity faces piercing of the corporate veil risk, regulatory fines, and joint-and-several liability for failures at the offshore entity level.

The foregoing set out what firms must do. The following section addresses how NCAs will likely enforce these requirements — and what firms may expect from the supervisory response.

NCA Supervisory Expectations: The Convergent Enforcement Model

ESMA has directed NCAs to coordinate closely and issued specific supervisory mandates. NCAs must: verify the existence and adequacy of orderly wind-down plans for unauthorised CASPs and ensure timely implementation without undue economic harm to clients; take enforcement action against the unauthorised provision of crypto-asset services in cooperation with other NCAs; scrutinise client migration strategies, ensuring authorised CASPs take timely steps to onboard EU clients from unauthorised CASPs including

group entities; ensure that unauthorised CASPs do not continue business-as-usual through group structures past the deadline and verify the “substance” of licensed CASPs — key personnel, compliance infrastructure, and mind-and-management must be genuinely located within the EU, not shells for offshore operators. By way of non-exhaustive overview

Jurisdiction	NCA	Key Position
Germany	BaFin	12-month transitional window: firms not authorised by end of December 2025 already out of time. January 2025 CASP circular published. Active enforcement via warnings, suspensions, and penalty orders. Has taken simultaneous action under MiCAR and securities prospectus law against single entities.
France	AMF	From 1 July 2026 only MiCAR-authorised CASPs may provide crypto-asset services. DASPs required to implement orderly cessation plans by 30 March 2026. Criminal penalties up to 2 years' imprisonment and €30,000 fine for post-deadline operation; administrative blacklisting and website blocking.
Spain	CNMV	Active supervisory reviews, spot checks, and investigations ongoing to confirm MiCAR compliance.
Italy	CONSOB	Active supervisory reviews, spot checks, and investigations ongoing to confirm MiCAR compliance.
Malta	MFSA	Active supervisory communications on end of transitional period and wind-down planning expectations.
Poland	KNF	Implementing legislation not in place by deadline. Entities under Polish transitional regime lose rights from 1 July 2026; must obtain CASP authorisation from another EU Member State and passport into Poland.
Luxembourg	CSSF	Active supervisory engagement on MiCAR authorisation pipeline and wind-down compliance for entities in the grandfathering regime.

A routine NCA inspection opens on three surfaces: client-asset segregation, conflicts policy in operation, and complaints handling. The CASP that has rebuilt the operating model can produce evidence on each within a working day. The CASP that has not, cannot — and the gap between those two outcomes is where supervisory action sits.

The preceding sections address regulatory exposure. Practitioners must also assess civil liability — both to clients and in insolvency. The following framework consolidates the principal heads of liability, their legal bases and (generic estimates of) risk levels.

Consolidated Liability Framework

Liability Head	Legal Basis	Key Points	Risk Level

Unauthorised operation	Art. 59 MiCAR; National law	Regulatory sanctions, management bans, civil claims for restitution and damages, potential criminal liability in some Member States	Very High
Statutory custody liability	Art. 75(8)	Loss of client assets attributable to CASP, capped at market value at time of loss. Cannot be contracted out of. Includes ICT incidents, fraud, key management failure, and sub-custodian failures. Price surges during operational failure expand liability symmetrically.	Very High
Client asset segregation failure	Art. 70	Use of client assets for own account, or failure to segregate. In insolvency: clients may become unsecured creditors rather than asset owners.	Very High
Wind-down failure	Art. 74; ESMA Apr 2026	Disorderly exit causing undue economic harm to clients. Forced liquidations, inadequate notice, withdrawal restrictions. Direct claims from clients for breach of custody duties and contractual damage.	Very High
Misleading or inadequate disclosure	Art. 66	Misrepresentation or omission in pre-contractual and ongoing communications. Tortious and contractual liability. Consumer protection violations. Particularly acute for retail clients.	High
Unsuitable advice / portfolio management	Art. 81	Inadequate suitability assessment plus resulting client loss. Follows MiFID II model. High-risk where documentation of client knowledge, objectives, and financial situation is absent.	High
Trading platform outage	Art. 76	Failed or delayed trades, erroneous liquidations. Claims for loss of opportunity, consequential damages, and contractual breaches.	High
Execution without consent / best execution failure	Art. 78; Q&A 2711	Off-platform execution without prior express client consent. Systematic failure to achieve best execution, particularly via affiliated venues.	High
Cyber incident	Art. 75; DORA	Client losses from hacking, theft, or malfunction. Attributable to CASP unless pure DLT protocol failure proven by CASP.	High
AML-related account freezes	AMLD; TFR	Regulatory compliance-driven asset restrictions; client claims for wrongful freezing.	Medium
Governance failures	Art. 68; Art. 74	Personal director/officer liability, management bans, insolvency actions.	High

GDPR violation on client migration	GDPR Art. 83	Mass data transfer to partner CASP without valid legal basis. Fines up to €20m or 4% of global annual turnover.	High

Key Risk Areas for Compliance

- **The pending application fallacy.** A filed but undecided application provides no continued operating rights after 1 July 2026. Continued activity in that position is a breach of EU law, not a grey area.

- **Intragroup structure risk.** Firms operating through EU-authorised entities but routing services, custody, or technology through non-authorised group entities face direct MiCAR exposure. The structure must follow the authorisation, not the brand. Intragroup fronting creates joint-and-several liability and piercing-of-veil risk.

- **Clean-sheet AML on client migration.** Any authorised CASP onboarding clients from an unauthorised entity — whether third party or group company — must conduct full, fresh customer due diligence. Inherited KYC files may not adequate.

- **Reverse solicitation is not a business model.** Post-ESMA's February 2025 guidelines, any form of digital presence characterised as EU-directed marketing disqualifies reliance on the exemption. Passive geo-blocking is necessary but not sufficient. Firms need documented evidence of client-initiated engagement at the individual transaction level. NCAs now deploy digital forensics, mystery shopping, and app store audits to detect violations.

- **The wind-down GDPR trap.** Bulk migration of client data to a partner CASP without valid legal basis — explicit consent or specific contractual necessity — violates GDPR. Fines of up to €20m or 4% of global turnover can consume remaining wind-down reserves. This is a widely underestimated risk.

- **The valuation trap in custody liability.** Article 75 caps liability at market value at the time of loss — not at fees paid. If a token's price surges during an operational failure, the CASP's balance sheet exposure expands symmetrically. Cyber-insurance must be sized against market value, not fees or nominal amounts.

- **Compliance is a continuously demonstrable operating model.** MiCAR CASP compliance is not a paperwork project that ends when the NCA returns the authorisation file. It is a continuously demonstrable operating model covering segregation, conflicts, ICT resilience, disclosure and client protection — tested at each inspection cycle.

- **Preferential treatment risk in wind-down.** Prioritising withdrawals for institutional clients, market makers, or insiders while retail client funds are delayed or frozen constitutes illegal preferential treatment. Bankruptcy liquidators will trigger clawback mechanisms. Directors face personal civil claims and potential criminal prosecution.

The liability framework above applies to CASPs and their management. Firms should also be aware of the position from the client’s perspective.

Warning for Consumers

ESMA wishes to warn investors engaging with crypto assets that not all providers are authorised under MiCAR after 1 July 2026, and that protections depend on who the investor is dealing with. Investors should verify their provider by checking whether the company is listed as authorised in the ESMA Interim MiCAR Register before investing or transferring funds. MiCAR protections only apply to the specific authorised legal entity in the EU — not to other companies of the same group, and not to non-EU entities. Although providers should serve EU clients through their EU-authorised entities only, they may operate under the same brand across multiple companies or countries; clients must review contracts carefully to confirm which entity is actually providing the service. If a provider is not authorised, ESMA is clear that "investors should act promptly — transfer crypto assets to an authorised provider or a self-hosted wallet or consider closing positions. Staying with an unauthorised provider may mean less legal protection and a greater risk of losing access to assets."

The analysis above sets out the regulatory and liability framework. The following section distils the immediate action points for authorised CASPs, unauthorised CASPs and their clients.

Practical Recommendations

For Authorised CASPs

- **Expedite remaining authorisation processes.** Where MiCAR authorisation applications remain pending, firms should engage proactively with their home NCA to accelerate the process. A filed but undecided application provides no continued operating rights after 1 July 2026; firms in this position must have contingency wind-down plans in place in parallel.

- **Conduct a full outsourcing and delegation audit.** Authorised CASPs should immediately review all outsourcing and delegation arrangements to confirm that no crypto-asset services — particularly custody — are being provided to EU clients through unauthorised entities, whether within or outside the group. An authorised CASP can only use another authorised CASP for sub-custody; using an unauthorised third-country custodian post-1 July is a direct breach, and the primary CASP remains 100% liable for any losses. Intragroup fronting — where the authorised EU entity acts as a conduit for an unauthorised offshore affiliate — creates piercing of the corporate veil risk, regulatory fines, and joint-and-several liability.

- **Rebuild client migration onboarding for regulatory resilience.** Full, fresh AML/CFT customer due diligence must be conducted for every migrating client; inherited KYC files from an unauthorised predecessor will not survive NCA scrutiny. Suitability and appropriateness assessments must be completed for all new clients receiving advisory or portfolio management services — churning migrating clients through generic onboarding flows without proper suitability assessment creates substantial exposure.

- **Ensure Article 75 custody liability is properly provisioned.** The near-strict liability regime under Article 75 caps liability at the market value of the crypto-asset at the time of loss — not at fees paid. Cyber-insurance policies must be aligned to this market-value cap rather than to a fees-based or fixed-sum formula. Contractual terms seeking to exclude Article 75(8) liability are void.

- **Prepare for NCA inspection readiness.** A routine NCA inspection opens on three surfaces: client-asset segregation, conflicts policy in operation, and complaints handling. Authorised CASPs should be able to produce evidence on each within a working day. Compliance is not a paperwork project that ends when the NCA returns the authorisation file; it is a continuously demonstrable operating model covering segregation, conflicts, ICT resilience, disclosure and client protection — tested at each inspection cycle.

- **Align governance notifications requirements[3].** Material changes to the application file — services, capital, governance or ownership etc. — require notification under Article 64 and in some cases fresh authorisation. Operators routinely miss this threshold, treating it as housekeeping when the supervisor reads it as the live application file.

- **Satisfy DORA operational resilience obligations.** CASPs must maintain appropriate ICT systems, business continuity plans, and incident management processes alongside DORA's ICT-specific requirements: incident classification frameworks, mandatory reporting timelines, and threat-led penetration testing for significant CASPs. NCAs review ICT architecture including intragroup reliance and sub-provider dependencies, with particular focus on custody functions.

For Unauthorised CASPs

- **Cease regulated services immediately on 1 July 2026.** The obligation to cease is unconditional. There is no further grace period or extension available. ESMA and NCAs are expected to take enforcement action in cooperation with each other where service provision continues.

- **Implement the wind-down plan without delay.** By 1 July 2026, any unauthorised CASP must have implemented its wind-down plan. The plan must be operational, credible, and immediately executable. ESMA treats last-minute disorderly exits as a supervisory failure, not a standard business closure. The AMF required DASPs to have plans operational by 30 March 2026 at the latest; any firm that has not done so is already in a supervisory failure position.

- **Ensure the wind-down budget is funded.** The firm must prove it has the capital to execute an orderly exit with zero incoming revenue. A dedicated standalone cash buffer — separate from daily operating capital — must cover infrastructure, legal fees, staff retention and blockchain gas fees. Prudential capital safeguards must be maintained under MiCAR Article 67 right up until the final client asset is successfully offboarded.

- **Prioritise client asset migration.** The plan must account for every client position through two-pronged offboarding: individual withdrawal to self-hosted wallets or bulk migration to a pre-vetted partner CASP actively listed on the ESMA Interim MiCAR Register. A "ghost account" protocol must be established for unresponsive users or unclaimed balances. For larger exchanges, tranche-based offboarding by asset tier or geographic region is required.

- **Avoid preferential treatment of clients during wind-down.** Prioritising withdrawals for institutional clients, market makers, or insiders while retail client funds are delayed or frozen constitutes illegal preferential treatment under Member State laws. Bankruptcy liquidators will trigger clawback mechanisms, and directors face personal civil claims and potential criminal prosecution.

---

[3] Commission Implementing Regulation (EU) 2025/306, Art. 4(3).

- **Maintain full regulatory compliance throughout wind-down.** KYC, transaction monitoring, and Travel Rule protocols must remain fully active for all outbound asset transfers throughout the wind-down window. The wind-down process cannot be exploited as an exit channel for illicit capital.

- **Address the GDPR data migration risk.** Porting user data to a partner CASP without a valid legal basis — explicit affirmative user consent or specific contractual necessity — violates GDPR and exposes the entity to penalties of up to €20 million or 4% of global annual turnover. Mass consent failures during client migration can consume remaining wind-down reserves.

- **Implement the reverse solicitation firewall.** Firms that wind down their EU entities but leave offshore parent websites accessible to EU traffic remain exposed. Hard geo-blocking of EU IP addresses must be implemented on all platforms and interfaces; EU app store presence must be removed; influencer and affiliate contracts must be updated to prohibit EU reach and onboarding previous EU users onto non-EU infrastructure during or after wind-down must be absolutely prohibited.

- **Boards and senior management must take personal responsibility.** Under Articles 68 and 74, executives carry direct fiduciary responsibility for ensuring an orderly exit. Personal exposure arises from continuing operations without authorisation, inadequate wind-down planning, misleading client disclosures about authorisation status, failure to safeguard client assets and insolvency-related misconduct. NCAs can issue multi-year professional bans preventing executives from holding management positions at any other EU financial or crypto institution.

For Clients and Investors

- **Verify your provider's authorisation status immediately.** Check that the company you are using is listed as authorised in the ESMA Interim MiCAR Register before investing or transferring funds. Not all providers will be authorised under MiCAR after 1 July 2026, and your protections depend on who you are dealing with.

- **Know exactly which legal entity is providing your service.** MiCAR protections only apply to the specific authorised legal entity in the EU — not to other companies of the same group, and not to non-EU entities. Although providers may operate under the same brand across multiple companies or countries, only the EU-authorised entity may serve EU clients. Review your contract carefully to confirm which entity is actually providing your service.

- **Act promptly if your provider is not authorised.** Transfer your crypto assets to an authorised provider or a self-hosted wallet, or consider closing your positions. Staying with an unauthorised provider may mean less legal protection and a greater risk of losing access to your assets.

- **Understand your strengthened legal position.** Clients of unauthorised operators are structurally advantaged in litigation. Contracts entered into by an entity providing regulated services without authorisation are in several Member States either void or voidable at the client's election, and multiple heads of claim are available including contractual invalidity, regulatory tort and illegality-based claims.

- **Confirm client asset segregation with your authorised CASP.** Under Article 70, authorised CASPs must make adequate arrangements to safeguard the ownership rights of clients, especially in insolvency, and must never use client assets for their own account. If segregation is ineffective in insolvency, clients may become unsecured creditors rather than asset owners.

- **Be aware of your rights under the Article 75 custody regime.** CASPs providing custody are liable for the loss of any crypto-assets attributable to them, capped at market value at the time of loss. Contractual terms seeking to exclude this liability are void. Article 75(4) also requires CASPs to credit clients with any new assets or rights arising from a hard fork, airdrop, or similar protocol event; failure to do so creates a direct client claim.

- **Insist on proper suitability assessments.** If you are receiving advisory or portfolio management services, your CASP must conduct a full suitability assessment taking into account your knowledge and experience, investment objectives, risk tolerance and financial situation. Advice without an adequate suitability assessment, resulting in loss, is a straightforward liability claim.

- **Utilise complaints procedures.** CASPs are required to establish effective and transparent complaints procedures, free of charge, with substantive responses within a reasonable timeframe. Exercising these rights creates a documented record that may be material in any subsequent regulatory or civil proceedings.

Outlook

The 1 July 2026 deadline carries implications beyond compliance. For authorised CASPs, the expiry of the MiCAR transitional period will reshape the competitive landscape as clients of unauthorised operators seek alternative service providers. The following considerations are relevant for authorised CASPs assessing their strategic positioning:

- **Client migration dynamics.** ESMA expects authorised CASPs to actively manage the migration of existing clients ahead of and after 1 July 2026. Clients currently serviced by unauthorised operators will need to transfer their assets to an authorised CASP or to self-hosted wallets. Given the operational complexity of self-custody, many retail and institutional clients are likely to seek onboarding with a licensed provider.

- **The MiCAR passport and cross-border access.** Authorised CASPs benefit from the single market passport — the ability to provide services across all 27 Member States from a single authorisation. This is the first time the EU crypto-asset market has operated under a genuinely harmonised cross-border framework, enabling authorised operators to serve clients across the EU without separate national registrations.

- **Market structure considerations.** MiCAR's prudential capital requirements (€50,000 to €150,000 minimum, plus the quarter-of-fixed-overheads dynamic requirement), governance obligations, operational resilience standards under DORA, and ongoing compliance infrastructure create barriers to entry that favour established, well-capitalised operators.

- **Regulatory status as a trust signal.** ESMA's consumer warning — directing investors to verify their provider against the ESMA Interim MiCAR Register — underscores the importance of authorised status. Clients who have experienced disruption from forced migration, or who have seen warnings about reduced legal protection with unauthorised providers, may place greater weight on regulatory certainty when selecting a service provider.

- **Institutional requirements.** The prohibition on outsourcing custody to unauthorised entities means that institutional allocators — asset managers, pension funds, family offices and corporate treasuries — can only deploy capital through authorised infrastructure. Firms that can demonstrate Article 70 segregation, Article 75 custody liability coverage and DORA-compliant operational resilience will be positioned to serve institutional clients with more stringent compliance requirements.

- **Third-country firm restrictions.** The prohibition on non-EU entities providing MiCAR services to EU clients — reinforced by ESMA's definition of solicitation and NCA audit methodologies — limits the ability of offshore platforms to serve EU clients directly. This regulatory framework applies uniformly to all market participants.

- **Transition timing.** The 30-to-90-day wind-down execution timeline creates a concentrated period during which clients of winding-down operators will seek alternative providers. Authorised CASPs should ensure their onboarding infrastructure and client support capacity can accommodate increased volumes during this period.

- **Operational considerations.** Authorised CASPs may wish to consider: ensuring onboarding processes are streamlined while satisfying fresh AML/CFT due diligence requirements; maintaining institutional-grade custody offerings that satisfy Article 75's liability standard with appropriate insurance coverage; and developing clear, consumer-friendly communications consistent with Article 66's requirement that communications be fair, clear and non-misleading.

Authorised CASPs that have invested in compliance infrastructure and operational resilience will be well-positioned to navigate the post-transition market. The regulatory framework is now settled, and the focus shifts to execution.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for the end of the MiCAR transitional period and related regulatory developments. We have assembled a multidisciplinary and multijurisdictional team of sector experts to support clients in navigating the challenges and seizing the opportunities presented by the evolving EU digital assets framework.

In relation to the MiCAR transitional period specifically, PwC Legal is providing:

- **Wind-down and transition planning.** Advice on the development and implementation of orderly wind-down plans for unauthorised CASPs, including client asset migration strategies, financial runway modelling, critical vendor mapping, compliance continuity and NCA notification protocols.

- **Client migration support for authorised CASPs.** Guidance on rebuilding onboarding processes for regulatory resilience, conducting full fresh AML/CFT customer due diligence and completing suitability and appropriateness assessments for migrating clients.

- **Outsourcing and delegation audits.** Review of outsourcing and delegation arrangements to confirm compliance with MiCAR’s prohibition on custody delegation to unauthorised entities, identification of intragroup fronting risks and remediation strategies.

- **Third-country firm compliance.** Advice on the reverse solicitation framework, geo-blocking implementation, app store and marketing compliance and post-wind-down firewall requirements for firms with non-EU operations.

- **NCA inspection readiness.** Preparation for NCA inspections, including client-asset segregation evidence, conflicts policy documentation, complaints handling infrastructure and governance notification compliance.

Moreover, we have developed a number of RegTech and SupTech tools for supervised firms, including PwC Legal's Rule Scanner tool, backed by a trusted set of managed solutions from PwC Legal Business Solutions, allowing for horizon scanning and risk mapping of all legislative and regulatory developments as well as sanctions and fines from more than 2,500 legislative and regulatory policymakers and other industry voices in over 170 jurisdictions impacting financial services firms and their business.

The PwC Legal Team behind Rule Scanner are proud recipients of ALM Law.com's coveted "2024 Disruptive Technology of the Year Award" and the "2025 Regulatory, Governance and Compliance Technology Award".

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via de_regcore@pwc.com or our website.

Contact

Dr. Michael Huertas
Tel: +49 160 97375760
michael.huertas@pwc.com

Dr. Hagen Weiss
Tel: +49 1511 5708446
hagen.weiss@pwc.com

EU RegCORE Team
de_regcore@pwc.com

www.pwc.de