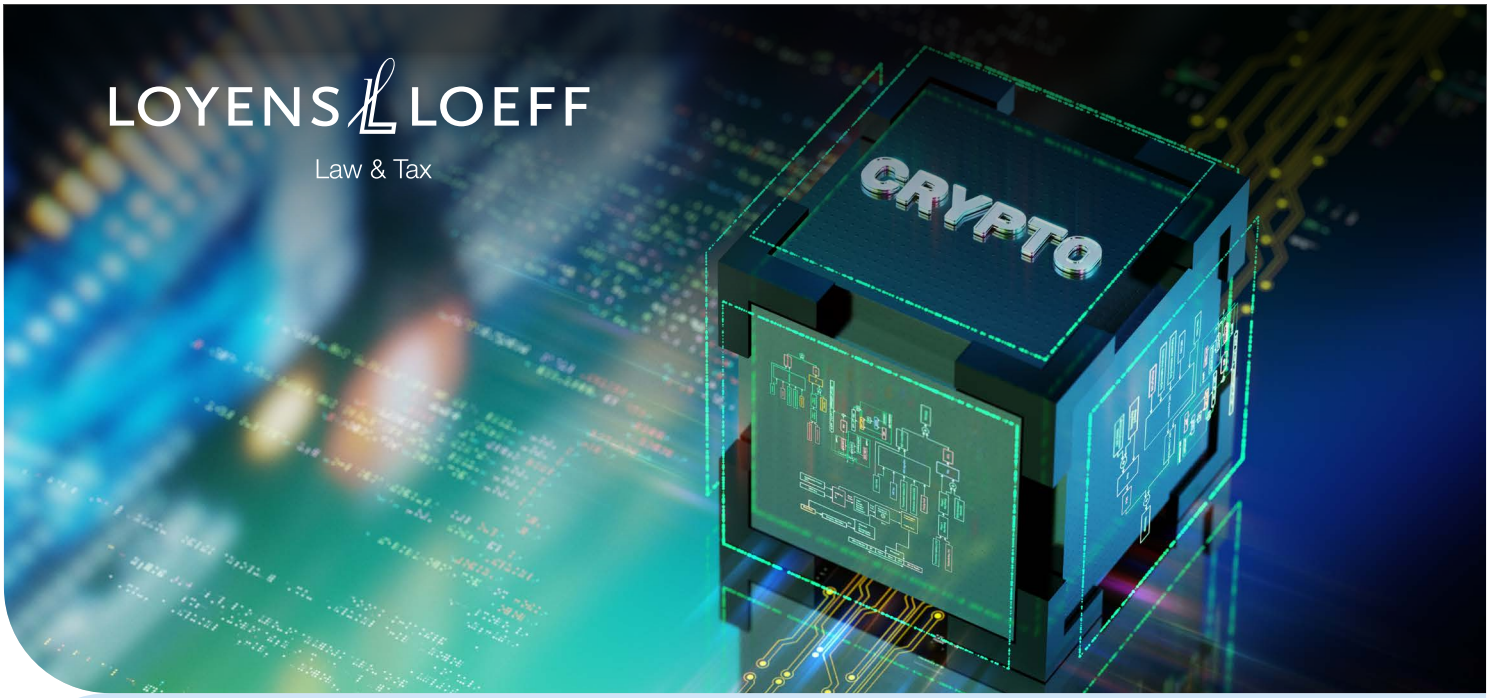
LOYENS & LOEFF
Law & Tax



Crypto M&A in Europe
10 Legal Recommendations

Crypto industry consolidation is accelerating under a tightening regulatory framework. In the EU and the Netherlands, new regulations (like MiCAR) and supervisory priorities (such as the 2025/2026 agenda of the AFM (as defined below)) are reshaping how crypto M&A deals must be executed. Below we outline ten key legal recommendations – focused on regulatory compliance and due diligence – to help acquirers and targets navigate crypto M&A in this evolving landscape.

1. Confirm MiCAR licensing status

Ensure that the target is properly licensed under the EU's Markets in Crypto-Assets Regulation (2023/1114) (**MiCAR**). As of 1 July 2026, MiCAR is fully applicable across all EU member states, and the transitional period for existing crypto-asset service providers (**CASPs**) has ended. Any CASP operating in the EU must now hold a MiCAR authorisation; operating without one constitutes a breach of EU law. The European Securities and Markets Authority (**ESMA**) has confirmed[1] that unauthorised CASPs must cease operations and implement orderly wind-down plans, including offboarding clients by transferring crypto-assets to an authorised CASP or to a self-hosted wallet. The end of the transitional period has triggered significant industry consolidation, with the majority of previously registered CASPs having exited the market.[2] In the Netherlands, the transitional period for previously registered crypto providers had already ended on 30 June 2025. The Dutch Authority for the Financial Markets (*Autoriteit Financiële Markten*, **AFM**) has since taken active supervisory steps against non-compliant firms. Acquirers should verify that the target company holds a valid MiCAR authorisation and is not subject to any pending enforcement or wind-down proceedings. Any absence of the required MiCAR authorisation should be treated as a critical deal issue.

1 ESMA Statement on the End of Transitional Periods under MICA, 17 April 2026, ESMA75-113276571-1679.

2 Transitional periods in EU member states differed – reference is made to: https://www.esma.europa.eu/sites/default/files/2024-12/List_of_MiCA_grandfathering_periods_art._143_3.pdf. The ultimate transitional deadline across the EU was 1 July 2026, and ESMA has confirmed that no further extensions are available.

2. Anticipate regulatory approval for acquisitions

Determine whether the proposed transaction triggers a "qualifying holding" notification under MiCAR. A qualifying holding refers – shortly put – to any direct or indirect stake in an issuer of asset-referenced tokens or a crypto-asset service provider that either (i) represents at least 10% of the company's capital or voting rights, including aggregated holdings, or (ii) gives the holder the ability to exert significant influence over the company's management. Under Article 83 of MiCAR, acquiring a qualifying holding in a CASP or increasing such qualifying holding so that the proportion of the voting rights or of the capital held in a CASP would reach or exceed 20%, 30%, or 50% or so that the CASP would become a subsidiary of the purchaser, requires prior notification and clearance from the competent authority of that CASP. This regime mirrors the approval process regarding the acquisition of a qualifying holding in banks or investment firms. In practice, the acquisition of a qualifying holding in a Dutch CASP requires a prior notification to DNB (*De Nederlandsche Bank N.V.*), along with the provision of extensive information regarding the purchaser's business, finances, and integrity. DNB will have up to 60 business days to assess the application (which can pause if additional information is requested), with an absolute maximum review period of 110 business days. Both the seller and the purchaser should factor this timeline into their deal planning as closing cannot occur until the competent authority formally approves. Early engagement is wise: start preparing the ownership change dossier (organizational charts, business plans, compliance records) as soon as deal talks get serious. Also note that MiCAR's approval requirement extends to acquisitions of issuers of asset-referenced tokens, not just CASPs. Failure to obtain the required approval could result in regulatory sanctions or nullify the transaction.

3. Prioritize AML and "travel rule" compliance

Anti-Money Laundering (**AML**) due diligence is paramount in any crypto acquisition. Verify that the target has strong AML procedures in line with EU and standards of the relevant EU member state (which may differ). In the Netherlands, CASPs have been subject to the Dutch AML Act (*Wet ter voorkoming van witwassen en financieren van terrorisme*), requiring KYC checks, suspicious activity reporting (under Dutch law: unusual transactions), and sanctions screening. Any lapses (e.g. missing DNB registration in the past, or prior enforcement actions) should be closely scrutinized. The AFM underscores that compliance with the AML Act and the Sanctions Act (*Sanctiewet 1977*) is a central supervisory pillar, and it is scrutinizing crypto firms' controls. The AFM has issued specific guidance that companies are required to follow, providing detailed expectations on AML and sanctions compliance for CASPs. Furthermore, as of late 2024, the EU's revised Transfer of Funds Regulation (2023/1113) (TFR) imposes the full "travel rule" on crypto transactions. This means that CASPs must attach identifying information for senders and recipients to crypto transfers (no minimum threshold, so effectively all transfers). By now (February 2026), the travel rule is in force – regulators expect firms to have implemented solutions for sharing originator/beneficiary data between CASPs. Ensure the target is compliant: have they integrated travel rule protocols or providers? Do they collect and transmit required customer data with transfers? Lack of travel rule compliance can lead to penalties. Similarly, check sanctions compliance: the firm should be screening customers and wallet addresses against EU sanctions lists and have controls for high-risk jurisdictions. Given the rising focus on preventing financial crime in crypto, both acquirer and target need to be confident that robust AML/CFT measures are in place and will hold up under regulatory scrutiny post-merger.

4. Assess regulatory classification of tokens and services

Map out how each of the target company's activities and crypto assets is regulated by MiCAR and any other laws or regulations and confirm the target company is in compliance. MiCAR covers most types of utility tokens and generally applies to crypto services. However, certain crypto-assets are outside MiCAR's scope or are in scope of MiCAR while being subject to other regimes. For example, a token that qualifies as a financial instrument (such as a security token) would be governed by MiFID II and applicable national securities laws, including EU prospectus and licensing requirements. Another example regards stablecoins. A stablecoin that qualifies as an 'e-money token' under MiCAR will be regulated primarily under the European E-Money Directive (and thus must be issued by an authorized credit institution or e-money institution, with applicable rules), while MiCAR adds further requirements such as a mandatory crypto-asset white paper and ongoing disclosure obligations, instead of regulating the token under MiCAR's general crypto-asset

regime only. If the target company has issued any token (through an ICO/IEO or otherwise), perform a legal analysis: is it within MiCAR's scope, or could it be considered a share, bond, unit in a collective investment, or a derivative? Ensure any necessary prospectuses or exemptions were done if it's a security, or that e-money tokens have the required authorisations. Similarly, if the target offers services like crypto lending, staking-as-a-service, or operates a DeFi platform front-end, consider emerging regulations and guidance (some of these activities might attract future oversight or fall under existing consumer finance laws). The acquirer should seek reps/warranties that no unlicensed regulated activity has been carried out. Essentially, no crypto product should lie in a grey zone: it either fits under MiCAR or other financial regulations. Identifying the correct classification will inform what licenses and compliance measures are needed. Missteps here can be costly (e.g. enforcement action for selling unregistered securities or unauthorized payment services), so resolve any ambiguities up front – possibly by obtaining regulatory opinions or comfort rulings where appropriate.

5. Include tax and assess tax reporting risks

In general, the principal objectives of tax due diligence include evaluating a target's historical tax compliance and interactions with tax authorities, identifying and quantifying specific risks that may lead to future assessments or corrections, and assessing transaction-specific tax considerations. From a compliance perspective, the crypto industry is subject to increasingly complex tax reporting obligations. Building on the regulatory definitions introduced under MiCAR, the latest amendment to the Directive on Administrative Cooperation (DAC8) brings a wide range of CASPs within scope of significantly expanded tax reporting and due diligence obligations. These obligations require CASPs to collect, validate, store, and report to the tax authorities certain personal and transactional data relating to their EU users. This information will then be automatically exchanged with other EU Member States and participating jurisdictions. Since DAC8 has been effective from 1 January 2026, tax due diligence should carefully assess the robustness of a target's DAC8 implementation framework, as well as any risks arising from incomplete, incorrect, or delayed compliance.

There are several additional material points of attention when conducting tax due diligence in the context of the acquisition of a CASP.

- First, deferred tax assets and liabilities should be carefully assessed and quantified. CASPs may maintain an operational crypto inventory as well as various other intangible assets, reflecting their highly technology-driven business models. An operational crypto inventory may expose CASPs to significant FX-like valuation risks, potentially resulting in deferred tax liabilities. In this context, tax due diligence should also assess the corporate income tax treatment and valuation of crypto-assets, including the consistency between accounting and tax treatment and the recognition of unrealised gains or losses.
- Second, where employee or management remuneration or bonus arrangements are granted in crypto-assets, the valuation of such crypto-assets should be properly assessed for wage withholding tax and reporting purposes.
- A third area of focus concerns withholding taxes (WHT). Given the highly digital and internationally dispersed nature of CASP business models, questions may arise regarding the adequacy of substance and economic presence. In certain cases, this may restrict eligibility for WHT exemptions on dividends and, in specific structures, potentially also on interest and royalty payments.
- Relatedly, tax due diligence should consider potential permanent establishment and transfer pricing risks arising from cross-border activities, the location of key decision-making functions, and the ownership and development of intellectual property.
- Another point of attention is VAT recoverability. Financial services are typically VAT-exempt, which limits the deductibility of input VAT. CASPs often provide a combination of VAT-exempt and VAT-taxable services, increasing the risk of overstated input VAT recovery and potential obligations to file supplementary VAT returns.

The points above are not exhaustive. Given the rapidly evolving regulatory and tax landscape applicable to CASPs, thorough and targeted tax due diligence is indispensable in any crypto-related M&A process.

6. Evaluate IT security and operational resilience

Cybersecurity and operational resilience are critical in crypto businesses – not only for business continuity, but also as a regulatory requirement (with frameworks like the EU Digital Operational Resilience Act (Regulation

2022/2554) (**DORA**) being applicable). Purchasers should assess the target company's IT infrastructure and obtain any available evidencing documentation. Under MiCAR, CASPs must have policies to safeguard client assets and promptly report incidents. If the target suffered past breaches, review how they were remedied and whether any competent authority and/or clients were notified. Also look at business continuity plans: can the platform sustain operations if a key system fails or if there's a sudden crypto market shock? Under DORA, in full effect since 17 January 2025, financial entities (including authorised CASPs and issuers of asset-reference tokens) must meet strict standards for recovery and testing of cyber defences. DORA also requires financial entities to maintain an ICT third-party register identifying all ICT service providers. Purchasers should therefore verify whether the target company's register is complete and up to date. Furthermore, any material post-closing changes to ICT service providers may trigger notification obligations under DORA, meaning that purchasers should plan for these reporting requirements as part of the integration process. Weaknesses in cybersecurity can be deal-breakers – a major undisclosed vulnerability or poor IT security might sway a purchaser to walk away or adjust the price. On the other hand, demonstrating strong IT security could support smoother deal execution and integration. Plan for an integration of IT systems post-closing that preserves security: for example, if the purchaser has more advanced security tooling, migrate the target company's systems to those standards swiftly. Given the AFM's focus on digitalisation risks (including cyber risks) in the financial sector, crypto M&A due diligence must treat tech risk on par with legal risk.

7. Check data protection (GDPR) and privacy practices

The target's handling of personal data should be fully compliant with the GDPR and any applicable GDPR national implementation acts (in the Netherlands the *Uitvoeringswet Algemene Verordening Gegevensbescherming*) as this is both a legal obligation and crucial for customer trust. Review the target company's available data protection and privacy related documents, such as privacy notices, a record of processing activities, consent mechanisms and data retention policies. Furthermore, verify if the target company has any history of data breaches; if so, were they (timely) reported to competent authorities and affected users as required by law? Also examine how the target company handles data subject requests (deletion, access requests) - an inability to fulfil these (in a timely manner) due to poor data management might indicate non-compliance. If the target transfers data outside the European Economic Area (e.g., using cloud services in the US or outsourcing support to India), ensure that proper safeguards are in place, given the stringent rules in that respect. An acquirer should plan to integrate the target's systems and databases in a way that maintains or enhances data protection (for example, unifying cybersecurity measures, and possibly conduct a Data Protection Impact Assessment (DPIA) if the merger changes the nature of data processing).

8. Scrutinise governance, personnel and "fit & proper" requirements

Good corporate governance and trustworthy management are essential, especially since regulators will do their own checks on these post-closing. A purchaser should examine the target company's governance structure: board composition, frequency of compliance committee meetings, and any internal audit or compliance reports. In the regulated crypto space, key individuals (board members, executives) must meet "fit and proper" criteria – basically demonstrating competence, experience, and integrity. As part of the deal, identify any directors or major shareholders who might not pass a regulatory vetting (e.g. due to prior bankruptcies, criminal records, or regulatory sanctions). It is a requirement under MiCAR to get approval for changes in management of the CASP, so plan for submissions of new directors' information to the regulator if leadership will change. Also consider retention of compliance-critical staff: the target's compliance officer or MLRO holds valuable institutional knowledge and relationship with regulators. The acquirer may want to secure key personnel through the transition to ensure continuity. Conversely, if due diligence reveals a weak compliance culture or a pattern of disregarding regulatory guidance, it signals a serious red flag—potentially requiring the swift replacement of key managers or a rapid overhaul of internal controls post-acquisition. The AFM and DNB have emphasized the "gatekeeper" role of financial firms in preventing abuses; having strong leadership in place who embrace that role will be crucial for the merged entity's long-term success. Ensure the deal agreement covers any needed commitments, like the seller assisting with regulatory notifications or certain founders staying on for a handover period to maintain market confidence.

9. Verify IP ownership and review key contracts

Make sure the target actually owns the intellectual property that is core to its operations. This includes software code (backend platforms, trading engines, smart contracts), proprietary algorithms, the website/app, the use of open-source software and any trademarks/brand names. In case the target developed software (or other relevant works), check employment and contractor agreements to confirm that any developers have assigned their IP rights in the results to the company – in startups, sometimes early code may have been created by founders or contractors without explicit IP assignment, which needs cleanup. If the platform uses open-source components, verify compliance with those licenses (to avoid, for example, a viral open-source license imposing unexpected obligations). Additionally, review whether use is made by any software of third-party materials and whether proper licenses have been maintained. Often in crypto partnerships with liquidity providers are entered into, API agreements with other platforms, banking and payment processing agreements, cloud service contracts, etc. Verify whether a change-of-control clause might require the other party's consent to the merger. Pay attention to any exclusivity or non-compete clauses the target may have agreed to – will the acquisition breach any exclusivity with a vendor or trigger any penalties? Also, check user terms of the target company's platform: do they allow assignment of user contracts to an acquirer and do the user terms comply with consumer protection regulations?

10. Plan post-merger integration and monitor regulatory developments

A successful crypto M&A doesn't end at closing – you need a post-merger plan focused on compliance integration and future-proofing the business.

Immediately after closing, align the target's compliance program with the acquirer's: update policies to the highest standard of the two firms, harmonize customer onboarding approaches, and integrate transaction monitoring systems. If the target company is rebranding or merging, remember to update its regulatory licenses/registrations accordingly and inform customers about any changes (like new terms or privacy notices reflecting the new owner). Keep a close watch on the horizon for regulatory changes.

The EU Anti-Money Laundering Authority (**AMLA**), operational since 1 July 2025 and based in Frankfurt, has already assumed EBA's former AML/CFT responsibilities and has identified crypto-asset services as a top money-laundering threat in the EU. AMLA will directly supervise approximately 40 high-risk financial institutions from 2028, including crypto firms, and is currently finalizing the methodology for its risk assessments. AMLA has specifically warned that the end of the MiCAR transitional period may create money-laundering risks as unauthorised firms exit the market and customer relationships are transferred to authorised providers at scale. This means acquirers should expect even tougher AML scrutiny and should ensure the target's compliance programme is robust enough to withstand AMLA's heightened supervisory expectations. Also, be aware of additional guidance under MiCAR that ESMA or EBA may issue – for instance on custody standards, sustainability disclosures for crypto (ESG), or treating DeFi interfaces.

On the Dutch front, the AFM published findings in April 2026[3] from a study of 33 CASPs, revealing significant shortcomings in advertising at 14 CASPs and in cost information at 19 CASPs, with supervisory letters issued to non-compliant Dutch firms. This underscores the AFM's active enforcement posture regarding crypto advertising and risk disclosures, and acquirers should ensure that the target's marketing materials and fee disclosures comply with MiCAR requirements. Plan for the merged company to proactively engage with regulators: consider scheduling an introductory meeting with the AFM/DNB post-acquisition to present your integration plan and demonstrate your commitment to compliance (this can build trust and potentially ease future processes). Finally, ensure that both parties preserve all relevant compliance documentation through the handover – regulatory inspections or audits can happen at any time, and being able to show a well-documented compliance history (even pre-acquisition) can be extremely valuable. By thoughtfully integrating and keeping ahead of legal developments, the newly merged business can turn regulatory compliance from a challenge into a competitive advantage, ensuring smooth operations across the EU. These post-merger obligations are primarily relevant where the transaction involves a merger, rebranding, or integration of existing operations; where a private-equity investor steps into an entity without any existing business activities, these post-closing issues generally do not arise.

3 AFM "Shortcomings in advertising and cost information for crypto parties", 16 April 2026: https://www.afm.nl/en/sector/actueel/2026/apr/pb-reclame-informatie-casps.

Contact

Should you require any assistance when considering any crypto M&A transaction in Europe, we are here to support you. Please contact your trusted adviser at Loyens & Loeff or one of our colleagues mentioned below.

Marcel Buur
Partner - Tax adviser
T +31 20 578 55 43
M +31 6 22 24 38 12
E marcel.buur@loyensloeff.com

Martijn Schoonewille
Partner - Attorney at law
T +31 20 578 57 35
M +31 6 51 86 27 25
E martijn.schoonewille@loyensloeff.com

Rob Schrooten
Partner - Attorney at law
T +31 20 578 54 37
M +31 6 53 42 70 18
E rob.schrooten@loyensloeff.com

Pjotr Heemskerk
Counsel - Attorney at law
T +31 10 224 61 53
M +31 6 10 93 90 12
E pjotr.heemskerk@loyensloeff.com

Sandrine Lekkerkerker
Tax adviser
T +31 20 578 58 75
M +31 6 83 20 33 47
E sandrine.lekkerkerker@loyensloeff.com

Wendy Pronk
Attorney at law
T +31 20 578 53 15
M +31 6 10 61 79 95
E wendy.pronk@loyensloeff.com