LOYENS LOEFF

Law & Tax

April 2025

Quoted

Crypto asset services:
MiCAR & DAC8

loyensloeff.com

Edition 166

In this edition

About Loyens & Loeff

Crypto asset services: MiCAR & DAC8

Executive summary

The EU regulatory landscape for crypto-assets is evolving with the introduction of two key regulations: MiCAR and DAC8. MiCAR seeks to harmonise the regulation of cryptocurrencies and digital assets across EU Member States. Being in effect as of 30 December 2024, MiCAR encompasses a broad range of crypto-assets and requires CASPs to obtain a license to legally operate in the EU. For those already registered as CASPs under the EU AML legislation, a transitional period with a maximum of eighteen months applies.[1] MiCAR also introduces rules for other players, such as market abuse rules and rules regarding the issuance and offering of crypto-assets, but these rules fall outside the scope of this Quoted. Next to MiCAR, and inspired on the OECD's CARF, DAC8 introduced a standardised EU reporting requirement coupled with an automatic exchange of information mechanism. DAC8 foresees new tax reporting obligations for providers of crypto-asset services (CASPs and CAOs), which are required to collect, validate, store and report to the tax authorities certain personal and transactional data about their EU users. Once reported, this data must then be automatically exchanged by EU Member States and countries implementing the OECD's CARF. Also encompassing CAOs, the scope of DAC8 is broader than that of MiCAR.[2] EU Member States have to transpose DAC8 into their national legislation by 31 December 2025, with the due diligence and reporting requirements taking effect as of 1 January 2026.

Introduction and background

The emergence of blockchain technology and crypto-assets has rapidly transformed the financial world. These technologies have not only created new financial opportunities but have also revolutionised the way in which financial transactions are carried out and information is stored. Inherent to such new developments is the adoption of relevant legislation, which in the European Union (**EU**) mainly concern the Markets in Crypto-Assets Regulation (**MiCAR**)[3] and the seventh amendment to the Directive on Administrative Cooperation (DAC), better known as DAC8.

Prior to the introduction of MiCAR, the provision of virtual or crypto-asset services was not regulated at the EU level, meaning that the provision of these services was generally and only subjected to the limited regulatory framework of the different EU Member States. Currently, in the Netherlands, certain crypto-asset service providers (**CASPs**), namely virtual currency exchange platforms and custodian wallet providers, operate under a registration regime provided for in the Dutch anti-money laundering legislation (i.e. the Dutch AML Act). Under this regime, virtual currency exchange platforms and custodian wallet providers have to comply with certain registration requirements and apply customer due diligence controls prior to providing any service. In most other EU Member States a similar regulatory regime applied to the provision of crypto-asset services prior to the introduction of MiCAR.

---

1   In the Netherlands, a transitional period of six months applies for parties which are already registered as crypto-asset service providers under the Dutch AML Act (*Wet ter voorkoming van witwassen en financiering van terrorisme*).
2   Please refer to paragraph 3.3.
3   Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.

MiCAR introduces a harmonised legal framework for crypto-asset markets within the EU. By introducing a harmonised licensing process for CASPs, MiCAR aims to facilitate the pursuit of crypto-asset business on an EU level and put an end to disparities between national regimes. MiCAR applies as of 30 December 2024, with certain provisions regarding the issuance and offering of asset-referenced tokens and e-money tokens being already applicable as of 30 June 2024.[4]

In the Netherlands, as in most jurisdictions, there are no specific tax laws on the substantive taxation of crypto-assets. The tax treatment of such assets is based on general principles and guidance issued by the Dutch Tax Authorities. For Dutch tax purposes, crypto-assets are not formally treated as money or liquid assets, but as (current) assets. As most corporate tax payers are deemed to conduct their business with all their assets, crypto-assets are deemed part of the business enterprise irrespective of the business it operates. This means that realised gains are taxed and losses are tax deductible. Crypto-assets on the balance sheet are valued at cost price or lower market value. If a corporate taxpayer receives payments in crypto-assets, these have to be converted to euros, or another functional currency if applicable.

Since today's tax laws were conceived/designed for traditional payment methods at a time when crypto-assets did not even exist, it is usual that the application of these existing legal frameworks leads to situations where there is no clear legal consequence following an action or transaction involving crypto-assets. As a result, governments and policymakers have taken steps to ensure that income from crypto-assets is reported and taxed adequately. Within the EU, the introduction of DAC8 is a significant development in this regard. DAC8 aims to facilitate enhanced cooperation among governments in the field of direct taxation, enabling more effective tax collection and combating tax fraud. The goal of DAC8 is to improve transparency and facilitate information exchange among EU Member States on crypto-asset transactions. In a nutshell, as of 2026, DAC8 obligates CASPs and

crypto-asset operators (**CAOs**) to annually collect, validate, store and report to the tax authorities certain personal and transaction data from their reportable clients. Once this data has been reported, the relevant information will be automatically exchanged between EU Member States and countries implementing the OECD's CARF.

This edition of Quoted addresses the key obligations faced by CASPs under MiCAR and DAC8 and their (practical) implications.[5] Following this short introduction, the document addresses the relevant topics in four chapters. Chapter 1 addresses the characteristics of various forms of crypto-assets and the underlying blockchain technology that enables the existence and exchange of this type of assets. In this chapter, we will also delve into the validation of crypto-asset transactions on a blockchain and the consensus mechanisms 'proof of work' and 'proof of stake'. Chapter 2 focuses on MiCAR in more detail. This chapter will, among other things, discuss the scope of the terms 'crypto-assets' and 'crypto-asset services', as well as the obligations that apply under MiCAR for such businesses. In chapter 3, an overview of the proposed DAC8 reporting obligations will be provided, including the responsible parties for reporting, the information to be reported, and potential complexities and challenges associated with its implementation. Chapter 4 will conclude with key attention points for businesses.

1.   Understanding crypto-assets and blockchain technology

1.1   Decentralisation and challenges in relevant legislation

One of the key features of crypto-assets is decentralisation. These digital assets operate without a central authority such as a government or central bank. This means they are immune to censorship and control by governments or financial institutions, providing a degree of financial autonomy to users. In terms of security, cryptography and blockchain technology - the foundation of most crypto-assets - make transactions secure and

---

4   Titles III and IV apply as of 30 June 2024. These titles describe the obligations in relation to the issuance of ARTs and EMTs.
5   In this Quoted, we will not focus on the rules for other market players, such as the market abuse rules and the rules in respect of the issuance and offering of crypto-assets.

transparent. This technology mitigates the risk of fraudulent activities related to the transactions themselves because they are essentially tamper-proof. As a result, users have trust in the system.

At the same time, a significant challenge of crypto-assets is regulatory uncertainty. Regulations surrounding crypto-assets are often still in their infancy and vary greatly from one country to another. This can be confusing for users, investors, and tax authorities. The lack of clear guidelines can lead to legal and tax issues. Furthermore, the anonymity that crypto-assets provide, although viewed as an advantage by some, can also lead to abuse. The use of crypto-assets for illegal activities, tax evasion, and other harmful purposes remains a point of concern for regulators and policymakers.

Decentralisation can vary in degree. Fully decentralised systems operate without intermediaries, relying solely on peer-to-peer networks and smart contracts. In contrast, most of the crypto market operates under a non-fully decentralised model, where CASPs act as intermediaries, centralising aspects of supply and demand. This partial centralisation allows regulators to impose tax reporting obligations on CASPs.

1.2   Blockchain technology

Blockchain technology serves as the backbone of crypto-assets. It operates as a public, digital ledger maintained by thousands of individuals, as opposed to a central bank or financial institution. The fundamental structure consists of what are called 'blocks' containing transactions, and these blocks are linked together to form a 'chain'; hence the name 'blockchain'.

A transaction on the blockchain works as follows:

1. **Recording transactions** - imagine an individual wants to send a crypto-asset to another person, this transaction is recorded in a new block.
2. **Reaching consensus** - before this new block is added to the chain, other users in the network must agree on the validity of the transaction. This consensus process is achieved through mechanisms such as 'proof of work' or 'proof of stake', which will be further explained in the next paragraph.

3. **Adding to the chain** - once the transaction is approved by the network, the new block is added to the blockchain. It not only contains this transaction but also references the previous block, creating an immutable chain.
4. **Distribution** - the blockchain is shared with all participants in the network, and everyone has a copy of the entire chain. This ensures transparency and security.

In addition to the decentralised nature of crypto-assets, the blockchain offers several advantages. Firstly, the technology provides security because the data on the blockchain is encrypted and difficult to alter. Secondly, it offers transparency because all participants can view the blockchain. Thirdly, it provides reliability because once recorded, data cannot be changed.

1.3   Validating crypto transactions

Referring to the previous paragraph, other users in the network must agree on the validity of transactions. The process of validating transactions and adding new blocks to the blockchain is also known as mining. This process plays a crucial role in maintaining the integrity of the blockchain.

The validation process differs depending on the consensus mechanism used. The two mechanisms most commonly used are 'proof of work' and 'proof of stake'.

- **Proof of work** - under the 'proof of work' concept, users compete to solve complex mathematical problems. The first user to find the correct answer adds a new block to the blockchain and is rewarded with new crypto-assets. As a result, solving the mathematical problem becomes more challenging as more mining occurs because more transactions need validation. Therefore, this process requires significant computational power and energy but enhances network security.
- **Proof of stake** - an alternative is the 'proof of stake' concept. Instead of competing, holders of crypto-assets validate transactions based on their stake or investment. The more crypto-assets you hold, the greater your chances of validating transactions and receiving rewards. Since it is not so much the user's computational power that matters for transaction validation, this concept is much more energy-efficient.

Both 'proof of work' and 'proof of stake' are consensus mechanisms that contribute to the integrity of the blockchain. The choice between 'proof of work' and 'proof of stake' will depend on the specific goals, preferences, and characteristics of the underlying blockchain project.

1.4   Different types of crypto-assets

Finally, as the range of crypto-assets is broad and can easily lead to different interpretations, it is essential to lay down some common definitions which will be used in this document. For this purpose, crypto-assets can generally be categorized into three types: payment tokens, utility tokens, and security tokens.[6]

- **Payment tokens** - payment tokens, such as Bitcoin, serve as digital currencies and are typically used as an alternative form of (digital) money. They have their own blockchain network and serve as means of exchange. Payment tokens are designed to function as a store of value.
- **Utility tokens** - utility tokens are often used to access specific services or features within a blockchain ecosystem. They serve a practical purpose and often represent a form of 'membership' within that ecosystem.
- **Security tokens** - security tokens represent traditional financial assets, such as stocks. They often grant holders rights to company shares or profit distributions.

While the concept of crypto-assets is a general one, there can be significant differences between them. In conclusion, payment tokens are digital currencies, while utility and security tokens can have a broader range of functions, including practical use or financial representation.

2.   Markets in Crypto-Assets Regulation (MiCAR)

2.1   Introduction

Following the big surge in the market capitalisation of crypto-assets during 2017, coupled with numerous cases of fraud and money laundering involving these assets, the necessity of an overall EU framework for markets in crypto-assets became increasingly apparent. In 2018, the European Commission tasked the European Banking Authority (**EBA**) and European Securities and Markets Authority (**ESMA**) with assessing the applicability and suitability of the existing EU financial services regulatory framework for crypto-assets.

The advisory report[7], issued in January 2019, highlighted that while certain crypto-assets may fall within the purview of EU legislation, effectively implementing regulations for these assets can be challenging. Furthermore, the report underscored that certain provisions within existing EU legislation might impede the utilisation of distributed ledger technology. At the same time, the EBA and ESMA underlined that - beyond EU legislation aimed at combating money laundering and terrorism financing - most crypto-assets fall outside the scope of EU financial services legislation and therefore are not subject to provisions on consumer and investor protection and market integrity, among others, although they give rise to these risks.

As part of the European Digital Finance package, which aims to enable and support the potential of digital finance in terms of innovation and competition, on 24 September 2020 the European Commission published a proposal for MiCAR. Following the legislative procedure, MiCAR entered into force on 29 June 2023 and applies as of 30 December 2024. The objectives of MiCAR are to enhance legal certainty in the field of crypto-assets that are not covered by the existing financial services legislation, to support innovation and fair competition, to promote the development of crypto-assets and use

6   See also P.Mell, N.Roby and K.Scarfone and D,Yaga, Blockchain Technology Overview, NISTIR 8202, 2018 and T. Lambert, D. Liebau, P. Roosenboom, Security token offerings, Small Business Economics, 2022.
7   EBA Report, 9 January 2019, "Report with advice for the European Commission on crypto-assets": https://www.eba.europa.eu/publications-and-media/press-releases/eba-reports-crypto-assets.

of distributed ledger technology, to protect consumers, investors and market integrity considering the risks associated with crypto-assets, and to ensure financial stability.

Under MiCAR a 'crypto-asset' is defined as "a digital representation of value or rights which may be transferred and stored electronically using distributed ledger technology or similar technology". Distinguishing among crypto-assets reveals three primary classifications.

- *Asset-referenced tokens* (**ARTs**) is a type of crypto-asset that is not an electronic money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies. The underlying assets backing ARTs can range from fiat currencies to commodities, real estate or other forms of value. Examples are Tether Gold (XAUT) backed by physical gold reserves, Tesla Stock Token (TSLA) representing fractional ownership of Tesla shares, or Real Tokens representing fractional ownership of real estate properties in the United States.
- *Electronic money tokens* (**EMTs**) (or e-money tokens) purport to maintain a stable value by referencing to the value of one official currency. EMTs represent digital equivalents of fiat currencies or other value-backed assets. Examples are USD Coin (USDC) or Tether (USDT), both pegged to the US dollar. In contrast to other payment tokens, such as Bitcoin, whose value fluctuates based on market supply and demand, EMTs are designed to maintain a stable value by being pegged to fiat currencies.
- *Utility tokens* serve the singular purpose of providing access to goods or services supplied by their issuer. Utility tokens can take various forms, including platform-specific tokens, gaming tokens, decentralized finance (DeFi) tokens, content creation and social media tokens, and more. For example, the Binance Coin (BNB) which provides access to certain services and discounts on the Binance exchange qualifies as a utility token.

Following the adoption of MiCAR, the whole crypto-asset industry in Europe is confronted with a new set of rules on:
- the transparency and disclosure requirements for the issuance and admission to trading of crypto-assets;
- the authorisation and supervision of CASPs and issuers of ARTs and issuers of EMTs;
- requirements for the protection of holders of crypto-assets in the issuance, public offering and admission to trading of crypto-assets;
- the protection of clients of CASPs; and
- market abuse to ensure the integrity of crypto-asset markets.[8]

For purposes of this Quoted, we will now further focus on the rules which apply to CASPs.

---

8   Article 1 MiCAR.

2.2   Crypto-asset services covered by MiCAR

The 'crypto-asset services'[9] covered by the MiCAR include the following:

Crypto-asset service	Explanation
Providing custody and administration of crypto-assets on behalf of clients	This service entails the safekeeping or controlling, on behalf of clients, of crypto-assets or of the means of access to such crypto-assets, where applicable in the form of private cryptographic keys.[10]
Operation of a trading platform for crypto-assets	This means the management of one or more multilateral systems, which bring together or facilitate the bringing together of multiple third-party purchasing and selling interests in crypto-assets, in the system and in accordance with its rules, in a way that results in a contract, either by exchanging crypto-assets for funds or by the exchange of crypto-assets for other crypto-assets.[11]
Exchange of crypto-assets for funds	This means the management of one or more multilateral systems, which bring together or facilitate the bringing together of multiple third-party purchasing and selling interests in crypto-assets, in the system and in accordance with its rules, in a way that results in a contract, either by exchanging crypto-assets for funds or by the exchange of crypto-assets for other crypto-assets.[12]
Exchange of crypto-assets for other crypto-assets	This service entails the conclusion of purchase or sale contracts concerning crypto-assets with clients for other crypto-assets by using proprietary capital.[13]

Crypto-asset service	Explanation
Execution of orders for crypto-assets on behalf of clients	This means the conclusion of agreements, on behalf of clients, to purchase or sell one or more crypto-assets or the subscription on behalf of clients for one or more crypto-assets, and includes the conclusion of contracts to sell crypto-assets at the moment of their offer to the public or admission to trading.[14]
Placing of crypto-assets	This service entails the marketing, on behalf of or for the account of the offeror or a party related to the offeror, of crypto-assets to purchasers.[15]
Reception and transmission of orders for crypto-assets on behalf of clients	This means the reception from a person of an order to purchase or sell one or more crypto-assets or to subscribe for one or more crypto-assets and the transmission of that order to a third party for execution.[16]
Providing advice on crypto-assets	This means offering, giving or agreeing to give personalised recommendations to a client, either at the client's request or on the initiative of the crypto-asset service provider providing the advice, in respect of one or more transactions relating to crypto-assets, or the use of crypto-asset services.[17]
Providing portfolio management on crypto-assets	This service entails the offering, giving or agreeing to give personalised recommendations to a client, either at the client's request or on the initiative of the crypto-asset service provider providing the advice, in respect of one or more transactions relating to crypto-assets, or the use of crypto-asset services.[18]
Providing transfer services for crypto-assets on behalf of clients	This means providing services of transfer, on behalf of a natural or legal person, of crypto-assets from one distributed ledger address or account to another.[19]

---

9   Article 3 (16) MiCAR.
10   Article 3 (17) MiCAR. This means the safekeeping or controlling, on behalf of clients, of crypto-assets or of the means of access to such crypto-assets, where applicable in the form of private cryptographic keys.
11   Article 3 (18) MiCAR.
12   Article 3 (19) MiCAR.
13   Article 3 (20) MiCAR.
14   Article 3 (21) MiCAR.
15   Article 3 (22) MiCAR.
16   Article 3 (23) MiCAR.
17   Article 3 (24) MiCAR.
18   Article 3 (25) MiCAR.
19   Article 3 (26) MiCAR.

2.3   Authorisation and obligations for CASPs

Under MiCAR, CASPs are subjected to authorisation requirements and general prudential requirements, rules on conduct of business, and governance requirements, as well as additional requirements that apply depending on the types of crypto-asset services being provided, such as the custody and administration of crypto-assets and the operation of a trading platform.[20]

The process for obtaining an authorisation is further detailed under MiCAR.[21] As part of the application process, amongst others information relating to the legal form of the entity, a description of the internal governance framework, programme of operations, policies and procedures, and the identity of shareholders will need to be communicated to the relevant competent authority. For the Netherlands, this is the Authority for the Financial Markets (**AFM**). Furthermore, the management body of the applicant CASP needs to have sufficiently good reputation and possess the appropriate knowledge, skills and experience to manage the CASP. Separately, the proposed acquirers holding a qualifying holding exceeding 20% require prior approval of the competent authority.[22] This process involves an assessment of the suitability and financial soundness of the proposed acquirer(s). Dependent on the type of services to be provided by the CASP, the AFM has a checklist available on its website with the information that should be provided as a minimum. [23]

The total statutory period for the competent authority to assess the license application is 105 working days, during which the approval of the proposed acquirers can be obtained. Once a CASP has obtained authorisation to provide crypto-asset services in a EU Member State, it may passport its authorisation in another EU Member State. The passporting regime allows the CASP to either provide services on a cross-border basis or via the establishment of a branch in another EU Member State.

Under certain conditions, regulated entities amongst which banks, investment firms, e-money institutions and AIFM's are allowed to provide crypto-asset services without the need to obtain an authorisation as a crypto-asset service provider under MiCAR.[24] In this case a simplified authorisation procedure applies to the relevant regulated entity wishing to add crypto-asset services to their existing services portfolio.

MiCAR explicitly recognises the concept of 'reverse solicitation' in relation to crypto-asset services[25], which is common in other financial services legislation such as Markets in Financial Instruments Directive II (MiFID II).[26] Where a client based in the EU initiates at its own exclusive initiative the provision of a crypto-asset service or activity by a third-country firm, the authorisation requirement under MiCAR will not apply to the provision of that crypto-asset service or activity. ESMA has consulted draft guidelines on the reverse solicitation exemption.[27] Under the draft guidelines, solicitation is to be given a wide meaning, capturing any type of marketing or offer through any medium and by any person, limiting the possibility to use the reverse solicitation possibility. Furthermore, the reverse solicitation exemption is intended to apply for a limited period and only in respect of the particular type of product or service requested by the client at its own initiative.

Once the authorisation has been obtained, similar to other types of entities in the financial sector, CASPs will be bound by prudential and organisational requirements.[28] These requirements are both general to all types of CASPs and there are specific

---

20   Title V Authorisation and operating conditions for crypto-asset service providers MiCAR.
21   Article 59 MiCAR.
22   In the Netherlands, this is DNB.
23   Further information can also be found on the website of the AFM: https://www.afm.nl/nl-nl/sector/cryptopartijen/vereisten-en-vergunningen/casp-notificatie.
24   Article 60 MiCAR.
25   Article 61 MiCAR.
26   Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.
27   Consultation Paper on the draft guidelines on reverse solicitation under the Markets in Crypto Assets Regulation (MiCAR), ESMA35-1872330276-1619, 29 January 2024.
28   Article 66 and further MiCAR.

requirements depending on the service provided (such as execution of orders, provision of advice or operating a trading platform). The requirements are inspired by the MiFID II legislation. Please refer to the table below for the essential obligations.

Prudential safeguards	Governance arrangements	Obligation to act honestly, fairly and professionally
CASPs are required to have prudential safeguards[29] equal to an amount of at least the higher of either: (i) the amount permanent minimum capital requirements, depending on the type of the crypto-asset services provided; or (ii) one quarter of the fixed overheads of the preceding year, reviewed annually. The prudential safeguards may take the form of either the CASP's own funds or an insurance policy or a combination thereof.	CASPs must have adequate governance arrangements with effective policies and procedures (e.g. IT/ business continuity, complaint handling, management of conflicts of interest, outsourcing)[30]. In relation to specific requirements, for example, CASPs providing advice on crypto-assets or providing portfolio management of crypto-assets shall assess whether the crypto-asset services or crypto-assets are suitable for their clients or prospective clients, taking into consideration their knowledge and experience in investing in crypto-assets, their investment objectives, including risk tolerance, and their financial situation including their ability to bear losses.[31]	CASPs are required to act honestly, fairly and professionally in accordance with the best interests of their clients and prospective clients.[32] Information provided must be fair, clear and not misleading and marketing communications must be identified as such. CASPs are under the obligation to warn clients regarding risks associated with transactions in crypto-assets. Also certain information must be publicly available, such as policies on pricing, costs and fees.

2.4   Administrative penalties and other measures

MiCAR encompasses provisions empowering national regulators to impose administrative penalties or other measures in instances where a CASP demonstrates non-compliance with obligations on the basis of MiCAR.[33] Such sanctions include, but are not limited to:

- publishing a statement indicating the CASP and/or the natural persons (i.e. directors or other de facto managers) responsible and the nature of the infringement;
- issuing an order requiring the CASP and/or the natural persons involved to end the infringement;
- withdrawal or suspension of the authorisation of the CASP;
- imposing administrative fines up to a maximum of EUR 5,000,000 or a % of the annual turnover of the CASP involved; and
- a temporary ban for members of the board or supervisory board of the CASP from performing managerial functions at CASPs.

MiCAR additionally prescribes the relevant circumstances which national competent authorities must consider when determining the level and type of measure, confirms the right of appeal for the CASP and the natural persons subject to the relevant measure, and specifies the circumstances under which a measure should be published.[34]

2.5   Complementary Anti-money laundering and Transfer of Funds Regulation

MiCAR is complemented by an anti-money laundering framework for the transfer of crypto-assets. This is achieved by extending the scope of the revised Wire Transfer Regulation (**WTR III**), also referred to as the Transfer of Funds Regulation, to the transfer of crypto-assets. The provisions of the WTR III entered into force on 29 June 2023 and apply from 30 December 2024 repealing the existing "revised Wire Transfer Regulation". The WTR

---

29   Article 67 MiCAR.
30   Article 68 MiCAR.
31   Article 81 MiCAR.
32   Article 66 MiCAR.
33   Article 111 MiCAR.
34   Articles 112, 113 and 114 MiCAR.

III entails the disclosure of relevant originator and beneficiary data (e.g. the name of the originator and beneficiary, the distributed-ledger address or crypto-asset account number, and the LEI code of another official identifier of the originator) for all crypto transfers without a minimum threshold (i.e. the so-called travel rule). Before making the crypto-assets available to beneficiaries, providers shall verify the accuracy of the information on the basis of documents, data or information obtained from a reliable and independent source, and that there are no risks of money laundering or terrorism financing.

The WTR III rules also cover transactions from so-called un-hosted wallets (i.e. a crypto-asset wallet address that is in the custody of a private user) when they interact with hosted wallets managed by CASPs. In case a customer sends or receives more than EUR 1,000, to or from their own un-hosted wallet, the CASP will need to verify whether the un-hosted wallet is effectively owned or controlled by this customer. The foregoing entails that CASPs will have to comply with the rules on the basis of the WTR III in case of any crypto-asset transfers.

Furthermore, all CASPs are in scope of the Dutch AML Act and the Dutch Sanctions Act 1977. Entities within scope of the Dutch AML Act (i.e. entities providing financial lease services as their principal business) should comply with the obligations as set out herein. Such obligations include inter alia mandatory client screening and reporting unusual transactions to the Financial Intelligence Unit - Nederland. The Sanctions Act 1977 requires entities amongst others to prevent any breach of applicable sanctions and report matches against the sanctions list. Under the Dutch AML Act and Sanctions Act, the AFM becomes the regulator of CASPs.

3. DAC8

3.1 Overview and purpose

Council Directive 2011/16/EU on administrative cooperation in the field of direct taxation (DAC) is one of the instruments that the EU designed to accommodate cooperation between Member States in the field of taxation. Among other things, this EU directive aims to facilitate the exchange of tax-related information among Member States to combat tax evasion and undesired forms of tax avoidance. Since the introduction of DAC, the directive has undergone several revisions to strengthen and modernize cooperation between Member States by extending the scope of information reporting and exchange in relation to several aspects.

In response to the growing importance of digital assets in the financial landscape, on 17 October 2023 the EU introduced a seventh amendment to the DAC which - among other measures - contemplates an EU standardised tax reporting framework and automatic exchange of information regarding crypto-assets (DAC8). As a consequence of DAC8, as of 1 January 2026, reporting CASPs and CAOs will have a legal obligation to annually comply with certain due diligence and tax reporting requirements in order to provide EU tax authorities with personal and transactional information about their clients and their transactions regarding crypto-assets.[35]

DAC8 is based on the OECD-developed CARF. In August 2022, the OECD approved the CARF and published it on 10 October 2022. Over 50 countries, including the Netherlands, have politically committed to participating in the CARF and exchanging cryptocurrency data. DAC8 clarifies that EU Member States must use the OECD commentary and the CARF as sources of clarification and interpretation to ensure uniform application between EU Member States (level playing field).

---

35   This also applies to non-EU CASPs and CAOs who have to register in the EU.

DAC8 covers CASPs and CAOs based in the EU and also those from non-EU countries that have a certain nexus with an EU country; for example, because they are effectively managed from an EU Member State or have a permanent establishment there. The Dutch implementation proposal has adopted this scope. We expect that, in practice, this will result in nearly all parties subject to the Dutch reporting obligations being those already regulated (i.e., the CASPs). Following the adoption of DAC8 in the Council, EU Member States are now obliged to implement the Directive in their domestic laws by the end of 2025. Several EU Member States have now begun the legislative process, including the Netherlands, where the public consultation on the national implementation of DAC8 was open from 24 October 2024 - 21 November 2024.[36]

3.2   Key provisions of DAC8

In a nutshell, under DAC8, providers of crypto-asset services are required to identify their clients through specific due diligence procedures (as outlined in paragraph 3.4 of this Quoted). These reporting providers of crypto-asset services are also obliged to determine the tax residency of their clients, which clients generally (will) provide through self-certification forms. Tax residency is an important element because information only needs to be reported for users of crypto-assets who are tax residents of an EU Member State or a non-EU country with which the respective Member State has concluded an agreement on automatic exchange of information.[37] In this regard, a switch-off mechanism applies. This mechanism prevents duplicate reporting obligations for non-EU providers of crypto-asset services in cases where a non-EU country already applies comparable reporting standards, such as the OECD's CARF. This means that if a non-EU country where a provider of crypto-asset services is established already complies with reporting requirements similar to those of DAC8 and effectively exchanges information about EU users with the relevant Member States, the reporting obligation in the EU can be

switched off for that specific non-EU provider. This so-called 'switch off' mechanism reduces administrative burdens for providers of crypto-asset services.

If a client is identified as a reportable user, the reporting provider of crypto-asset services must collect, review and report all relevant information to the tax authorities of the Member State of registration, including personal client information and detailed transaction data, which is then exchanged with the tax authority of the country in which the crypto user is tax resident.

3.3   Providers of crypto-asset services

If it is determined that crypto-asset services are being offered (please refer to paragraph 2.2 of this Quoted), the provider of these services may be subject to the due diligence and reporting requirements of DAC8. These obligations apply to both CASPs and to CAOs, the latter term being introduced by DAC8.[38]

- **Crypto-asset service provider** (CASP) - this means a legal person or other undertaking whose occupation or business is the provision of one or more crypto-asset services to clients on a professional basis, and that is allowed to provide crypto-asset services in accordance with article 59 MiCAR.[39]
- **Crypto-asset operator** (CAO) - this means a provider of crypto-asset services other than a crypto-asset service provider.[40]

For purposes of DAC8, the CAO serves as a catch-all provision; when a provider of crypto-asset services is not already within the scope of MiCAR, they are likely to be subject to the reporting obligation of DAC8. Practically, this means that not only CASPs regulated under MiCAR are covered under DAC8, but also providers of crypto-asset services that are not regulated under MiCAR (as they are then classified as CAOs).

---

36   But also, for example, Czech Republic, France, Lithuania, Germany, Slovak Republic, Spain and Denmark.
37   The obligations arising from the CARF apply if both jurisdictions have informed the coordinating secretariat of the OECD that they wish to exchange information.
38   This is therefore not a definition that can be found in MiCAR.
39   Article 3, paragraph 15, MiCAR.
40   Section IV.B paragraph 2, annex III, DAC.

It should be noted that a provider of crypto-asset services is only subject to the DAC8 reporting requirements if this provider has a nexus with the EU. A nexus of this kind exists if an entity has obtained a license in an EU Member State under MiCAR or is allowed to offer crypto-asset activities in a Member State (see also paragraph 2.3 of this Quoted).

Even in cases where there is no authorisation under MiCAR, a nexus with the EU can still exist. This occurs if a provider of crypto-asset services (i) is an entity or natural person who is a tax resident in a Member State, (ii) is an entity established under the law of a Member State, (iii) is an entity that is effectively managed from a Member State, (iv) is an entity or natural person that has a regular place of business in a Member State, or (v) conducts reportable transactions through a branch in a Member State.

3.4   Due diligence procedure

If a provider of crypto-asset services falls under DAC8, it will need to establish for each client whether it is a reportable user. This is done through a due diligence procedure, of which the steps involved can be summarized as follows:

Step 1 - determine if the client is an individual crypto-asset user
If the client is an individual crypto-asset user, the reporting obligations of DAC8 apply if this individual has indicated on the self-certification form that he is a tax resident in an EU Member State.

If the client is identified as an entity crypto-asset user, it must be determined whether the entity is an excluded person.

Step 2 - determine if the entity is an excluded person
An excluded person is defined as: (i) an entity whose shares regularly traded on one or more established securities markets and any affiliated entity; (ii) a government entity; (iii) an international organization; (iv) a central bank; or (v) a financial institution, such as a custodian, a deposit-taking institution, an investment entity, or a specified insurance company. If an entity is identified as an excluded person, the reporting obligations of DAC8 do not apply to this entity.

If the client is identified as an entity that is not an excluded person, the next step must be followed.

Step 3 - determine if the entity is an active entity
DAC8 includes a framework to determine whether an entity is considered an active entity. This is a comprehensive framework, but in essence, an entity will at least meet the definition of an active entity if its activities consist of generating active business income, i.e. income other than interest, royalties, dividends, rent etc., which is considered passive income.

If an entity is classified as an active entity, the reporting obligations of DAC8 apply if this active entity has declared on a self-certification form that it is a tax resident in an EU Member State.

If determined that a client is not an active entity, the latter automatically fall into the residual category. Like an active entity, the reporting obligations of DAC8 apply to this entity if it has declared on a self-certification form that it is a tax resident in an EU Member State. Additionally, for this residual category, there is an additional reporting requirement: in addition to the entity itself, the ultimate beneficial owners must also be reported, provided they are tax residents in the Netherlands or an EU Member State.

The above will also apply to the extent that clients - or ultimate beneficial owners - are tax residents in a country outside the EU with which the relevant Member State has concluded an agreement for the automatic exchange of information regarding crypto-assets.

3.5   Reportable crypto-assets

For the purposes of DAC8, the terms 'crypto-assets' and 'reportable crypto-assets' are defined as follows:

- **Crypto-asset**: means a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology.

- **Reportable crypto-asset**: means any crypto-asset other than a central bank digital currency, electronic money, or any crypto-asset for which the reporting crypto-asset service provider has adequately determined that it cannot be used for payment or investment purposes.

The definition of crypto-assets is broadly formulated. Moreover, from the above, it can be concluded that the classification as a crypto-asset under MiCAR does not necessarily mean that this crypto-asset is subject to the reporting obligation of DAC8. As a definition of a reportable crypto-asset under DAC8, it applies to any crypto-asset other than a central bank digital currency (CBDC) or electronic money. In this regard, it should be considered that the exemptions provided in MiCAR, such as for certain closed-loop tokens and certain utility tokens, apply in this context. At the same time, there are crypto-assets that do not qualify as such under MiCAR but do fall under the reporting and information disclosure requirement of DAC8. This is the case with non-fungible tokens (NFTs), for instance, as well as any other crypto-asset that falls outside the scope of the MiCAR definition, but for which the reporting provider of crypto-asset services has adequately determined that it can be used for payment or investment purpose.

3.6   Reportable transactions and transfers

DAC8 does not specify a particular date by which reporting crypto-asset service providers must report. This means that EU Member States must make their own decision on this matter. In the Netherlands, the government has proposed 31 January of the calendar year following the year or period for which the report must be made as the latest reporting date. Under the CARF, reporting CASPs must conduct due diligence on their customers by 31 December.[41]

Reporting providers of crypto-asset services will need to provide personal data of the reportable users.[42] In addition, a significant amount of transaction data needs to be reported.[43] For each crypto-asset, all purchases and sales need to be reported. This includes details such as the units bought and sold, as well as the gross amounts paid and received (expressed in fiat currency). By providing this detailed information, local tax authorities should be better able to verify residents' tax returns. However, whether this is actually the case will largely depend on how EU Member States tax the use of or trading in crypto-assets; the way in which crypto-assets are taxed varies across EU Member States and depends on the specific national legislation of each individual EU Member State.

For the reporting obligations of DAC8, roughly three different types of transactions can be identified:

---

41   See Part III, Section A, CARF.

42   Article 8ad, paragraph 3, sub a DAC: the name, address, Member State(s) of residence, TIN(s) and, in the case of an individual, date and place of birth of each Reportable User and, in the case of any Entity that, after application of the due diligence procedures laid down in Section III of Annex VI is identified as having one or more Controlling Persons that is a Reportable Person, the name, address, Member State(s) of residence and TIN(s) of the Entity and the name, address, Member State(s) of residence, TIN(s) and date and place of birth of each Controlling Person of the Entity that is a Reportable Person, as well as the role(s) by virtue of which each such Reportable Person is a Controlling Person of the Entity.

43   Article 8ad, paragraph 3, sub c DAC: for each type of Reportable Crypto-Asset with respect to which the Reporting Crypto-Asset Service Provider has effectuated Reportable Transactions during the relevant calendar year or other appropriate reporting period, where relevant: (i) the full name of the type of Reportable Crypto-Asset; (ii) the aggregate gross amount paid, the aggregate number of units and the number of Reportable Transactions in respect of acquisitions against Fiat Currency; (iii) the aggregate gross amount received, the aggregate number of units and the number of Reportable Transactions in respect of disposals against Fiat Currency; (iv) the aggregate fair market value, the aggregate number of units and the number of Reportable Transactions in respect of acquisitions against other Reportable Crypto-Assets; (v) the aggregate fair market value, the aggregate number of units and the number of Reportable Transactions in respect of disposals against other Reportable Crypto-Assets; (vi) the aggregate fair market value, the aggregate number of units and the number of Reportable Retail Payment Transactions; (vii) the aggregate fair market value, the aggregate number of units and the number of Reportable Transactions, and subdivided by transfer type where known by the Reporting Crypto-Asset Service Provider, in respect of Transfers to the Reportable User not covered by points (ii) and (iv); (viii) the aggregate fair market value, the aggregate number of units and the number of Reportable Transactions, and subdivided by transfer type where known by the Reporting Crypto-Asset Service Provider, in respect of Transfers by the Reportable User not covered by points (iii), (v) and (vi); and (ix) the aggregate fair market value, as well as the aggregate number of units of Transfers effectuated by the Reporting Crypto-Asset Service Provider to distributed ledger addresses referred to in Regulation (EU) 2023/1114 not known to be associated with a virtual asset service provider or financial institution.

1. **Exchange transactions between crypto-assets and fiat currency** - this transaction involves swapping crypto-assets (e.g., Bitcoin) for traditional fiat currency (e.g., USD, EUR). Such transactions are common on crypto exchanges, where users can buy or sell crypto with national currencies. For example, someone might exchange Bitcoin for euros when cashing out profits from their investments.

2. **Exchange transactions between one or more crypto-assets** - in this case, one crypto-asset is exchanged directly for another. For instance, an investor may swap Ethereum (ETH) for Solana (SOL) on a crypto exchange platform.

3. **Transfers of crypto-assets** - transfers refer to moving crypto-assets from one wallet or address to another, often without any exchange for fiat or other crypto-assets. This is common for sending funds between personal wallets or paying others directly in crypto. For example, a user might transfer Bitcoin from their exchange account to a secure personal wallet for (long-term) storage.

In any case, transactions will be reportable if a crypto-asset is disposed of against either fiat currency (point 1) or against one or more crypto-assets (point 2). However, even if a different type of transfer occurs, there may be a reportable transaction. This can be the case, for example, when a crypto-asset is transferred from one account to another without an immediately identifiable consideration. This may apply, for instance, in the case of airdrops, staking, or lending.

3.7   Penalties

DAC8 requires Member States to provide for sanctions that are effective, proportionate, and dissuasive. In its original draft, the DAC8 proposal aimed to harmonise penalties across EU Member States. It introduced a structured system of minimum penalties for non-compliance with DAC8 reporting obligations, including for CASPs and CAOs who failed to provide accurate or complete data. However, this proposal was deleted in the final DAC8 proposal. The implementation of the sanctions is left to the individual EU Member States. This means that each Member State is responsible for defining and implementing such sanctions within its national legislation.

In the Netherlands, non-compliance can result in a fine from the sixth category. This entails a fine of up to EUR 1,030,000 (2025) if there is intent or gross negligence. The Dutch government considers the maximum of the sixth category to be sufficiently deterrent. Furthermore, this maximum aligns with the existing limits applicable to obligations implemented under the previous DACs. For these reasons, the Dutch government deems a fine of up to the amount of the sixth category appropriate. This maximum also provides room to impose a proportionate fine. What constitutes a proportionate fine depends on all relevant facts and circumstances of the specific case.

4.   Key attention points

4.1   MiCAR

Following the adoption of MiCAR, the whole crypto-asset industry in the EU faces a new regulatory landscape. The new regulatory framework encompasses transparency and disclosure requirements for the issuance and admission to trading of crypto-assets, the authorisation and supervision of CASPs and issuers of ARTs and EMTs, requirements for the protection of holders of crypto-assets in the issuance, public offering and admission to trading of crypto-assets, the protection of clients of CASPs, and market abuse to ensure the integrity of crypto-asset markets. For purpose of this Quoted, we focused on the rules that apply to CASPs. In our view, the following general points merit attention:

- **Licensing process** - MiCAR took effect on 30 December 2024, requiring entities to obtain a license as a CASP by that date. For parties currently registered as crypto-asset service providers with the Dutch Central Bank (*De Nederlandsche Bank N.V.*, **DNB**) under the Dutch AML Act, a transitional period of six months applies. In the Netherlands, the AFM is the competent authority responsible for handling license applications. The application process opened on 22 April 2024. The statutory period for the AFM to assess a license application is 105 working days, during which time approval of the proposed acquirers can also be obtained. Once the licensed is obtained, CASPs must maintain prudential safeguards, comply with certain organisational requirements and conduct of business rules.

- **Convergent application of MiCAR** - important to note for market parties is that the EU legislator puts emphasise on the importance of MiCAR being applied consistently within each of the Member States. One of the issues identified in this respect is the different approaches to national transposition of MiFID II across Member States. Against that background, ESMA has published guidance on the qualification of crypto-assets as financial instruments.[44] Furthermore, the European Supervisory Authorities have published a standardised test for the classification of crypto-assets.[45] Separately, ESMA encourages national competent authorities to look into the business model of market parties combining a broad range of crypto-asset services and products, centred around the operation of a trading platform, to avoid that part of the activities of the group will not be regulated.[46]
- **Overlap with other EU legislation** - due to new business models evolving and the newly regulated crypto-environment, overlap may exist between MiCAR and other pieces of legislation. This may for instance be the case for the provision of payment services and crypto-asset services, especially where it concerns the issuance of EMTs. In a letter of 6 December 2024[47], the EU Commission highlights the differing interpretations among Member States regarding the interaction between MiCAR and the Payment Services Directive II (2015/2366/EU (**PSDII**). It requests that the EBA, in collaboration with ESMA, consider issuing a "no action letter" to address the enforcement of PSDII authorization requirements for services involving electronic money tokens provided by crypto asset service providers or entities benefiting from MiCAR's transitional period, which might unintentionally fall under PSDII. Additionally, the Commission suggests that if dual authorisation is still necessary, the EBA and ESMA should explore ways to streamline the PSDII authorisation process to lessen the operational burden on institutions.

4.2   DAC8

The DAC has been amended for the seventh time. The key changes of DAC8 for CASPs and CAOs relate to determining the scope of application of the due diligence and reporting rules foreseen therein, as well as the collection and exchange of data regarding crypto-assets and their users. EU Member States have until 31 December 2025 to transpose the Directive into national law. The relevant DAC8 provisions will come into effect on 1 January 2026.

As highlighted in this edition of Quoted, CASPs and CAOs need to be prepared for the upcoming legislation. In our view, the three main general points of attention are as follows:

- **Scoping** - CASPs and CAOs may face difficulties in determining the crypto-assets in scope based on the subjective and discretionary classification of crypto-assets. Reporting providers of crypto-asset services must independently assess whether a crypto-asset qualifies as a reportable crypto-asset. This is the case if the crypto-asset can be used for payment or investment purposes. Each reporting provider of crypto-asset services must therefore make this assessment independently. As of this moment, there is very little guidance on how this should be determined. The obvious risk is that each provider of crypto-asset services across the EU may give a different qualification to (the same) crypto-asset.
- **Performing due diligence procedures** - for individuals and entities providing crypto-asset services, it is important that they (i) are required to identify their customers, (ii) determine in which country they are tax residents, and (iii) collect reportable information about their customers according to specific due diligence procedures. It is possible that the reporting CASPs and CAOs already collect this data to a certain extent and are able to provide it to the local authority. For any missing information,

---

44   ESMA Draft Consultation paper on the draft Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments ESMA75-453128700-52.
45   Draft Guidelines on templates for explanations and opinions, and the standardized test for the classification of crypto-assets, under Article 97(1) of Regulation (EU) 2023/1114 of 12 July 2024 (ESA 2024 12).
46   ESMA Opinion to support the convergent application of MiCAR, 31 July 2024 (ESMA75-453128700-1048).
47   Letter of European Commission of 6 December 2024, via: https://www.eba.europa.eu/sites/default/files/2024-12/3225040c-5f3d-410f-9156-f06a43231938/Letter%20to%20EBA%20and%20ESMA%20on%20the%20interplay%20between%20MiCA%20and%20PSD2.pdf.

a self-certification form should be provided to existing clients. For new customers, such self-certification can be provided during the onboarding process. To comply with the DAC8 requirements, CASPs and CAOs must determine which users are tax residents within the EU or tax residents of a country outside the EU which has an equivalent reporting regime and with which the relevant Member State has an agreement on the automatic exchange of information and effectively exchanges information.

- **Technological adaptations and security measures** - the reporting CASPs and CAOs must report the personal information of the reportable users, as well as detailed transaction data, annually to the relevant EU Member State with which they have a nexus. EU Member States will then exchange this information annually on an automatic basis. Since the information must be provided starting from 2026, a third important point of attention is that each reporting provider of crypto-asset services needs to make sure that internal processes and procedures are set up in order to collect and report the required information.
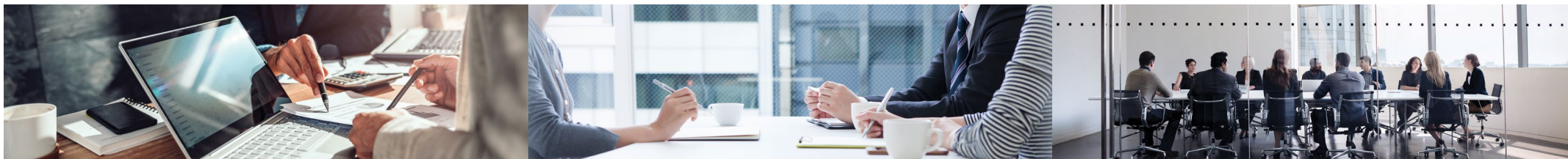
About Loyens & Loeff

Loyens & Loeff N.V. is an independent full service firm of civil lawyers, tax advisors and notaries, where civil law and tax services are provided on an integrated basis. The civil lawyers and notaries on the one hand and the tax advisors on the other hand have an equal position within the firm. This size and purpose make Loyens & Loeff N.V. unique in the Benelux countries and Switzerland.

The practice is primarily focused on the business sector (national and international) and the public sector. Loyens & Loeff N.V. is seen as a firm with extensive knowledge and experience in the area of, inter alia, tax law, corporate law, mergers and acquisitions, stock exchange listings, privatisations, banking and securities law, commercial real estate, employment law, administrative law, technology, media and procedural law, EU and competition, construction law, energy law, insolvency, environmental law, pensions law and spatial planning.

LOYENS LOEFF

Law & Tax

One Firm: Law & Tax, we are proud of the unique service we offer multinational enterprises, financial institutions, investors and High Net-Worth Individuals from our home markets of the Netherlands, Belgium, Luxembourg and Switzerland. With offices in key financial centres and a global partner network, we reach out and support you wherever you need.

As a leading law & tax firm in continental Europe, we have a particular focus on Private Equity & Funds, Real Estate, Life Sciences & Healthcare and Energy & Infrastructure. We integrate tax, civil law and notarial expertise to support you with smart and efficient solutions through advice, transactions and litigation.

As a trusted partner, the best advice is not just about expertise, but also about cultivating an in-depth understanding of your business and finding the best solution for you. This commitment is fundamental to our success.

Join us in going **Further. Better. Together.**

Amsterdam, Brussels, London, Luxembourg, New York, Paris, Rotterdam, Tokyo, Zurich

loyensloeff.com