Understanding and Implementing DAC8 & Crypto-Asset Reporting Framework (CARF)

2025 Update

About Taxbit

Taxbit's expert-built platform automates information and financial reporting across borders, currencies, and jurisdictions – seamlessly integrating for scalable, effortless compliance.

An End-to-End Tax and Accounting Platform for Digital Assets

The premier end-to-end compliance and reporting solution for the digital economy. Our single API-powered platform for tax and accounting reduces manual work to improve operational efficiency.

Tax Information Reporting

Stay compliant with global regulations and simplify your reporting process for customer transaction data. Taxbit's information reporting tools automate the ingestion of data and generation of required tax forms.

Accounting and Financial Reporting

With powerful tools, simplify and automate your digital asset accounting. Taxbit's subledger solution integrates with your existing systems to categorize transactions, generate financial reports, and seamlessly update your general ledger.

Taxbit is trusted by leading enterprises and governments

PayPal
kraken
FOX
wise
KPMG
GEMINI
Google
BINANCE
ZeroHash
uphold

Introduction

On October 10, 2022, "In light of the rapid development and growth of the Crypto-Asset market," the Organization for Economic Co-operation and Development (OECD) published the final guidance for the Crypto-Asset Reporting Framework (CARF) and Amendments to the Common Reporting Standards (CRS). Since then, many resources have been published to offer guidance on CARF implementation for both participating jurisdictions as well as Crypto-Asset Service Providers (CASPs). Resources include:

The OECD's Official CARF XML Schema

The Global Forum's Capacity-Building Strategy

The Global Forum's Step-by-Step Guide to Understanding and Implementing CARF

On 17 October 2023, the European Council adopted EU Directive 2023/2226 amending Directive 2011/16/EU on administrative cooperation in the field of taxation (DAC). DAC8 represents the EU's adoption of OECD's Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard. Member states have until December 31, 2025 to transpose the DAC8 reporting obligation into their domestic law and are required to give effect to those provisions as of January 1, 2026.

Under the framework, Reporting Crypto-Asset Service Providers (RCASPs), including exchanges, wallet providers, and potentially some DeFi platforms, are obligated to report transaction data. Further, they have a broad scope covering a wide range of crypto-assets and transactions, aiming for comprehensive oversight of crypto activity. It's crucial to understand the underlying implications of this new reporting framework. The primary objective of these frameworks is to achieve tax transparency across jurisdictions through annual exchanges of information related to crypto transactions.

In this article, we'll delve into the key aspects of these frameworks, exploring who is affected, what needs to be reported, and what steps stakeholders should take to prepare. Understanding these elements is essential for anyone involved in the crypto space to ensure compliance and navigate the evolving regulatory environment.

Understanding the DAC8 and CARF Regimes

Entities That Fall Into Scope for Reporting

Reporting Crypto-Asset Service Providers (RCASPs) must report relevant customer and transaction data to the appropriate jurisdictions. RCASPs include any entity or individual that facilitates crypto transactions as part of a business. This includes crypto exchanges, wallet providers, brokers, and financial institutions dealing with crypto-assets. Even decentralized finance (DeFi) platforms that provide transaction facilitation services may qualify as RCASPs, depending on their role in transactions. Businesses that solely provide software or hardware for crypto transactions, however, are generally not considered RCASPs.

Relevant Crypto-Assets

The definition for relevant crypto-assets is generally quite broad. "**Crypto-asset**" is defined as "a digital representation of value that relies on a cryptographically secured distributed ledger or similar technology to validate and secure transactions."

Assets not subject to reporting:

1. **Central Bank Digital Currencies:** A Central Bank Digital Currency is any digital fiat currency issued by a central bank, and is specifically excluded because it's included in the scope of the CRS

2. **Specified Electronic Money Products:** Specified Electronic Money Product represents a single fiat currency and that is redeemable at any time in the same fiat currency, and is specifically excluded because it's included in the scope of the CRS.

3. **Crypto-Assets which cannot be used for payment or investment purposes**

To assess whether a crypto asset cannot be used for payment or investment purposes, the CARF commentary specifically addresses the following three categories:

1. **"Closed-loop" Ecosystem:** Assets that can only be exchanged or redeemed within a limited fixed network or environment cannot be used for payment or investment purposes. An example of a closed-loop asset would be a loyalty reward program, such as airline miles or rewards points redeemable only with the rewarding entity. This can also apply to digital music, games, books or other media, as well as tickets, software applications and online subscriptions, as long as the Crypto-Assets cannot be transferred or exchanged on a secondary market.
2. **Crypto-Assets that represent Financial Assets:** Such assets are in-scope for CARF because they can be used for payment or investment purposes. Examples include tokenized equities, real-estate, and other asset-backed tokens.
3. **Non-Fungible Tokens (NFTs):** The OECD determined that in many instances NFTs are marketed as collectibles, but this function does not prevent an NFT from being used for payment or investment purposes. NFTs should be evaluated on a case-by-case basis taking into consideration the nature of the NFT and its function in practice to determine whether they can be used for payment or investment purposes.

Entities That Fall Into Scope for Reporting

A reportable user under the framework is a crypto-asset user, which is defined as a customer of the RCASP that is carrying out reportable transactions. Both entities and individuals will fall into a reportable user definition. However, it is important to note that the following types of users are specifically excluded from the scope:

- Public companies
- Governmental entities
- International organisations
- Central banks
- Financial institutions

What Types of Transactions Are Covered?

The following are in scope for reporting:

- ➔ **Crypto-to-fiat exchanges**, such as buying or selling Bitcoin for USD or Euros.
- ➔ **Crypto-to-crypto trades**, such as swapping Ethereum for Litecoin.
- ➔ **Reportable Retain Payment Transactions**, where the value of the transaction exceeds $50,000 USD
- ➔ **Any other transfer of crypto-assets**, including (but not limited to) transfers to and from self-hosted wallets

The first two categories are easy to understand as they are common activities seen on cryptocurrency exchanges. Information on buy, sells, and trades will be required to be tracked at the transactional-level in order to be able to report the required information accurately in the aggregate. This will require RCASP's to implement solutions that track asset pricing at the time of the transaction, report user's aggregate acquisition obtainment value, and report the aggregate proceeds generated on the platform.

Under the third category, payment processors that facilitate crypto-based retail or merchant transactions exceeding $50,000 USD will be required to collect information and report on the transaction. Implementation of this reporting will require data collection at the point of sale by the payment processor in order to report on the customer.

The fourth category requires the broadest of all, requiring any other type of transfer to be reported. Most notably, RCASPs will be required to identify if a transfer off-platform is going to another CASP or a self-hosted wallet. Data must be collected and reported anytime crypto-assets are transferred to an external crypto-asset address that is not associated with another Reporting CASP. In some ways this rule overlaps with the FATF's Travel Rule for digital assets. It also overlaps with the recent reporting legislation passed in the US that requires brokers to report to the IRS certain information about the transfer of digital assets to non-brokers. This type of transaction reporting is novel from a tax compliance standpoint because it expands reporting to non-taxable transactions.

Certain crypto assets may be transferred to and held by taxpayers in "cold wallets" (a way to hold cryptocurrency offline), which are not associated with a CASP or other financial institution. In order to increase visibility on these types of transfers, the CARF will require reporting at the aggregate level for transfers by a CASP to a user's cold wallet.

CARF & DAC8 Differences

DAC8 has a handful of key differences that are important for RCASPs to understand.

➔ **Restriction of Customer Activity:** If a customer does not provide the required self-certification after two (2) reminders from the RCASP within 60 days, the RCASP must block the customer from performing reportable transactions on the platform.

➔ **Extraterritorial Reach:** RCASPs authorized to perform crypto-asset services under MiCA are already registered in the EU and therefore subject to DAC8 in their member state(s) of residence. In addition, non-EU based RCASPs that perform crypto-asset services in the EU are also pulled into scope for DAC8 reporting. Non-EU RCASPs with EU branches or customers will need to register and report in a Member State. It should be noted that if the RCASP is submitting a report under CARF in a partner jurisdiction that has agreed to share information with the EU, this should satisfy the reporting requirement under DAC8 without the need to file in multiple locations.

➔ **GDPR Notifications:** RCASPs must inform each concerned customer that information relating to this individual will be collected and reported to the competent authorities at the latest before the information is reported.

➔ **Penalties:** DAC8 proposes penalties for non-compliance ranging between EUR 20’000 and EUR 500’000.

Participating Jurisdictions & Next Steps

As of early 2025, 63 jurisdictions have committed to implementing the CARF, with the first reporting to take place in either 2027 or 2028. The European Union has formally adopted DAC8 and EE countries are working towards compliance.

The implementation timeline is structured to allow jurisdictions and businesses ample time to prepare. Between **2025 and 2026**, jurisdictions will focus on passing legislation, building compliance frameworks, and setting up IT infrastructure. RCASPs likewise need to establish due diligence procedures and build the infrastructure needed to collect and report on relevant data.

By **2027 and 2028**, the first reporting cycle will begin. RCASPs need to be prepared to submit annual reports to local tax authorities, and tax authorities will begin to exchange crypto-transaction data.

Crypto businesses that qualify as RCASPs must take proactive steps now to ensure compliance with the DAC8 and CARFrequirements beginning in 2026:

- ➔ Implement enhanced onboarding procedures to ensure the collection of self-certifications.
- ➔ Prepare their IT systems to collect, store, and report transaction data securely, ensuring that they meet regulatory requirements without compromising user privacy.
- ➔ Understand any local registration and filing requirements that must be completed prior to submitting the first jurisdictional filing.

How Taxbit Can Help

Taxbit for DAC8/CARF is expertly designed for RCASPs - offering a crypto-native, enterprise-grade platform to automate reporting and streamline compliance. With seamless self-certification, secure data handling, and automated end-to-end reporting, Taxbit helps RCASPs stay compliant without disrupting their user experience.

Frictionless Self-Certification

Taxbit's drop-in SDK streamlines onboarding, allowing users to self-certify tax residency data effortlessly. This ensures compliance from the start of the user journey, protecting brand trust, without complicating onboarding.

Secure, Adaptive Data Handling

Taxbit protects sensitive information with advanced, end-to-end encryption, fully compliant with GDPR and SOC II standards. Our in-house tax and technical experts work behind the scenes to keep your compliance seamless and up-to-date as regulations evolve.

Automated, End-to-End Reporting

Taxbit's integrated platform automates every step of compliance—from transaction tracking to audit-ready regulatory reporting. The single dashboard provides a centralized view for real-time data validation and seamless oversight.

With Taxbit, RCASPs can turn regulatory complexity into operational simplicity—ensuring compliance across borders, jurisdictions, and currencies.

PayPal kraken FOX wise

KPMG GEMINI Google BINANCE

ZeroHash uphold

www.taxbit.com

Follow us on Twitter X

Follow us on LinkedIn