Guidance on reporting obligations of Reporting Crypto-Asset Service Providers

Part 38-03-38

This document should be read in conjunction with section 891HA and section 891M of the Taxes Consolidation Act 1997; OECD (2023), International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 update to the Common Reporting Standard; Crypto-Asset Reporting Framework: Frequently Asked Questions; European Union (Administrative Cooperation in the Field of Taxation) Regulations 2012 (as amended) and Council Directive (EU) 2023/2226 of 17 October 2023 amending Directive 2011/16/EU on administrative cooperation in the field of taxation.

Document created August 2026

Table of Contents

1 Introduction

The Crypto-Asset Reporting Framework (CARF)[1], developed by the Organisation for Economic Co-operation and Development (OECD), is the agreed standard for the collection and automatic exchange of information on crypto-asset transactions between tax administrations.

CARF was developed to address the rapid growth of the crypto-asset market by ensuring that relevant information on crypto-asset transactions is collected and reported in a consistent manner across jurisdictions[2].

CARF introduces new reporting obligations for reporting crypto-asset service providers (RCASPs), together with the automatic exchange of that information between participating jurisdictions.

Within the European Union, these measures are given effect through amendments to the Directive on Administrative Cooperation[3] (DAC). The DAC was amended by Council Directive (EU) 2023/2226 (commonly referred to as "DAC8") and gives effect to the CARF framework within the European Union.

This guidance is based primarily on the CARF framework, supplemented where necessary by the specific provisions of DAC8 that apply within the European Union.

In Ireland, the obligations imposed on RCASPs by CARF and DAC8 are provided for in the following legislation –

- Section 891HA of the Taxes Consolidation Act 1997 ("TCA1997")[4]
- Section 891M of the Taxes Consolidation Act 1997[5];
- OECD (2023), International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 update to the Common Reporting Standard;
- European Union (Administrative Cooperation in the Field of Taxation) Regulations 2025 - S.I. No. 584 of 2025;
- European Union (Administrative Cooperation in the Field of Taxation) Regulations 2012 (as amended); and
- Council Directive (EU) 2023/2226 of 17 October 2023 amending Directive 2011/16/EU on administrative cooperation in the field of taxation.

[1] OECD (2023), International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 update to the Common Reporting Standard

[2] Introduction to the CARF

[3] Council Directive 2011/16/EU

[4] Section 891HA TCA 1997, inserted by section 92 Finance Act 2025

[5] Section 891M TCA 1997, inserted by S.I. No. 584 of 2025

The reporting obligations placed on RCASPs by CARF and DAC8 apply from 1 January 2026. The purpose of this Tax and Duty Manual is to provide general guidance on the operation of the reporting obligations of RCASPs in Ireland.

2 Overview and key definitions[6]

CARF and DAC8 build on a set of clearly defined terms to ensure consistency, transparency, and alignment in reporting across jurisdictions including all Member States. These definitions establish what qualifies as a crypto-asset, who is considered a reporting entity and what constitutes a reportable transaction. This section outlines these definitions and provides additional information to help crypto-asset service providers understand how the rules apply in practice.

For each definition, this section explains the meaning under CARF and DAC8 and highlights where the terms have the same meaning under the CARF and DAC8 or where there are differences. The definitions should be read together, as many of them build on each other and are needed to understand how the reporting obligations apply.

2.1 Relevant crypto-asset / Reportable crypto-asset

2.1.1 "Crypto-asset"

A crypto-asset is defined in CARF as a digital representation of value that relies on a cryptographically secured distributed ledger or a similar technology to validate and secure transactions.

Within the European Union, the regulatory framework for crypto-assets is set out in Regulation (EU) 2023/1114 on Markets in Crypto-Assets[7] (commonly referred to as the MiCAR). DAC 8 aligns with the CARF definition of crypto-assets and applies it in an EU context, taking into account the key definitions and terminology of the MiCAR[8].

[6] Section IV of Part I (2. Rules) of the CARF and Annex IV of the DAC, which was inserted by Annex III of Council Directive (EU) 2023/2226 of 17 October 2023, provide a number of definitions pertaining to CARF and DAC8 and should also be consulted.

[7] DAC8 defines "crypto-asset" in Article 3(1), point (5), of Regulation (EU) 2023/1114

[8] MiCAR introduced a new regulatory framework for crypto-assets. S.I. No. 607/2024 - European Union (Markets in Crypto-Assets) Regulations 2024 gave effect to MiCAR and had a commencement date of 8 November 2024. The Central Bank is the National Competent Authority for carrying out the functions and duties provided for in the MiCAR. MiCAR registered CASPs (crypto-asset service provider) have a requirement to register and report as an RCASP (reportable crypto-asset service provider) in Ireland.

2.1.2 "Relevant crypto-asset" / "Reportable crypto-asset"

Under CARF, a relevant crypto-asset means any crypto-asset other than:

- a Central Bank Digital Currency (CBDC)[9],
- a Specified Electronic Money Product[10], or
- any crypto-asset that the RCASP has adequately determined cannot be used for payment or investment purposes.

DAC8 uses the term "reportable crypto-asset" which corresponds to the concept of a "relevant crypto-asset" under CARF.

CARF and DAC8 specifically exclude the reporting of CBDCs and electronic money because these instruments are already accounted for within existing financial account and payment frameworks and are expected to be reported, where relevant, under DAC2-CRS[11], thereby avoiding duplication within the CARF and DAC8 crypto-asset reporting regime. Section I of Part 2 - Rules of the CARF provides more comprehensive guidance on the CARF registration requirements.

Examples of crypto-assets include (but are not limited to):

- Cryptocurrencies (e.g. Bitcoin, Ethereum)
- Utility Tokens (tokens used for specific services)
- Security Tokens (tokens that represent ownership in an asset)
- Stablecoins (tokens that are tied to real-world money)
- Fungible tokens (tokens that are interchangeable with one another)
- Non-Fungible Tokens (unique digital items)
- Derivatives (contracts that can be exchanged for real money or other crypto-assets).

Not all crypto-assets listed above will necessarily be relevant / reportable crypto-assets for the purposes of CARF and DAC8. The reportability of a crypto-asset depends on whether it falls within the scope of the reporting rules and whether it is subject to any applicable exclusions[12].

---

[9] "Central Bank Digital Currency" means any digital Fiat Currency issued by a Central Bank.

[10] "Specified Electronic Money Product" means any crypto-asset that is: (a) a digital representation of a single Fiat Currency; (b) issued on receipt of funds for the purpose of making payment transactions; (c) represented by a claim on the issuer denominated in the same Fiat Currency; (d) accepted in payment by a natural or legal person other than the issuer; and (e) by virtue of regulatory requirements to which the issuer is subject, redeemable at any time and at par value for the same Fiat Currency upon request of the holder of the product.

[11] FATCA/DAC2-CRS

[12] Further details and examples are available in Part 3 (Commentary to the Rules) of the CARF.

2.2 Reporting crypto-asset service provider

2.2.1 "Crypto-asset service"

Unlike DAC8, CARF does not define the term "crypto-asset service". Instead, CARF applies to any individual or entity that, as a business, provides a service that effectuates transactions in crypto-assets for or on behalf of customers.

In the European Union, DAC8 operates within the MiCAR, which defines a crypto-asset service as any of the following services and activities relating to any crypto-asset[13]:

a. providing custody and administration of crypto-assets on behalf of clients[14];
b. operation of a trading platform for crypto-assets[15];
c. exchange of crypto-assets for funds[16];
d. exchange of crypto-assets for other crypto-assets[17];
e. execution of orders for crypto-assets on behalf of clients[18];
f. placing of crypto-assets[19];
g. reception and transmission of orders for crypto-assets on behalf of clients;[20]

[13] Article 3(1), point (16) of Regulation (EU) 2023/1114

[14] "providing custody and administration of crypto-assets on behalf of clients" 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; Article 3(1), point 17, of Regulation (EU)2023/1114

[15] "operation of a trading platform for crypto-assets" 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; Article 3(1), point 18, of Regulation (EU) 2023/1114

[16] "exchange of crypto-assets for funds" means the conclusion of purchase or sale contracts concerning crypto-assets with clients for funds by using proprietary capital; Article 3(1), point 19, of Regulation (EU) 2023/1114

[17] "exchange of crypto-assets for other crypto-assets" means the conclusion of purchase or sale contracts concerning crypto-assets with clients for other crypto-assets by using proprietary capital; Article 3(1), point 20, of Regulation (EU) 2023/1114

[18] "execution of orders for crypto-assets on behalf of clients" 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; Article 3(1), point 21, of Regulation (EU) 2023/1114

[19] "placing of crypto-assets" means the marketing, on behalf of or for the account of the offeror or a party related to the offeror, of crypto-assets to purchasers; Article 3(1), point 22, of Regulation (EU) 2023/1114

[20] "reception and transmission of orders for crypto-assets on behalf of clients" means the reception

h. providing advice on crypto-assets[21];
i. providing portfolio management on crypto-assets[22];
j. providing transfer services for crypto-assets on behalf of clients[23];
k. staking[24];
l. lending.

2.2.2 "Crypto-asset service provider"

CARF does not define "crypto-asset service provider" but does define "reporting crypto-asset service provider" as outlined in section 2.2.4.

DAC8 defines a crypto-asset service provider as 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, is authorised to provide crypto-asset services in accordance with the MiCAR[25] and has reporting obligations under DAC8.

2.2.3 "Crypto-asset operator"

DAC8 introduces the concept of a crypto-asset operator and defines a crypto-asset operator as a provider of crypto-asset services other than a crypto-asset service provider.

---

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; Article 3(1), point 23, of Regulation (EU) 2023/1114

[21] "providing advice on crypto-assets" 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; Article 3(1), point 24, of Regulation (EU) 2023/1114

[22] "providing portfolio management of crypto-assets" means managing portfolios in accordance with mandates given by clients on a discretionary client-by-client basis where such portfolios include one or more crypto-assets; Article 3(1), point 25, of Regulation (EU) 2023/1114

[23] "providing transfer services for crypto-assets on behalf of clients" 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; Article 3(1), point 26, of Regulation (EU) 2023/1114

[24] Section IV of Council Directive (EU) 2023/2226

[25] Article 3(1), point (15), of Regulation (EU) 2023/1114

[26] Nexus for CARF and DAC8 purposes means that an RCASP has a connection to a jurisdiction or Member State based on a hierarchy of (a)residence, (b)incorporation, (c)management, (d)regular place of business or (e) a branch.

[27] "Branch" means a unit, business or office of an RCASP that is treated as a branch under the regulatory regime of a jurisdiction or that is otherwise regulated under the laws of a jurisdiction as separate from other offices, units or branches of the RCASP. All units, businesses or offices of an RCASP in a single jurisdiction shall be treated as a single branch.

For the purposes of DAC8, a crypto-asset operator will be within scope where it has a sufficient nexus[26] to a Member State, including where it is:

(a) an entity or individual resident for tax purposes in a Member State;

(b) an entity that:

(i) is incorporated or organised under the laws of a Member State, and

(ii) either has legal personality in a Member State or has an obligation to file tax returns or tax information returns to the tax authorities in a Member State with respect to the income of the entity;

(c) an entity managed from a Member State; or

(d) an entity or individual that has a regular place of business in a Member State.

In addition, an RCASP that carries out reportable transactions through a branch[27] in Ireland is required to comply with the DAC8 due diligence and reporting obligations in Ireland.

This ensures that reporting obligations apply to both crypto-asset service providers regulated by and authorised under the MiCAR and to crypto-asset operators that are not. Both are referred to as reporting crypto-asset service providers (RCASPs), as they are required to report under DAC8.

2.2.4 "Reporting crypto-asset service provider"

Under CARF, a reporting crypto-asset service provider (RCASP) is any individual or entity that, as a business, provides a service effectuating relevant transactions for or on behalf of customers, including by acting as a counterparty, or as an intermediary, to such exchange transactions, or by making available a trading platform.

For the purposes of DAC8, an RCASP includes:

- any crypto-asset service provider regulated by and authorised in Ireland under the MiCAR, and
- any crypto-asset operator conducting one or more crypto-asset services for or on behalf of a reportable user that results in an exchange transaction and has a nexus to a Member State as outlined in section 2.2.3.

2.3 Relevant Transaction / Reportable Transaction

Under CARF, a relevant transaction means any one or combination of:

a. an exchange of relevant crypto-assets and fiat currencies[28],

[28] A "Fiat Currency" is the official currency of a country and is issued by the country's government or Central Bank. This currency can be in the form of physical banknotes or coins, or in digital forms, including bank reserves and central bank digital currencies. The term also includes commercial bank money and electronic money products (e-money). A stablecoin that qualifies as a Specified Electronic Money Product is treated as fiat currency.

b. an exchange between one or more forms of relevant crypto-assets,
c. a transfer of relevant crypto-assets, or
d. a reportable retail payment transaction.

A reportable retail payment transaction means a transfer of relevant crypto-assets in consideration of goods or services for a value exceeding USD 50,000, or equivalent in local currency.

DAC8 uses the term “reportable transaction” and captures the same categories of transactions as those defined under CARF.

An exchange includes the movement of a relevant crypto-asset from one wallet address to another, in payment for another relevant crypto-asset or fiat currency.

A transfer means a transaction that moves a relevant crypto-asset from or to the crypto-asset address or account of one crypto-asset user, including transfers to external wallets. It does not include transfers between accounts held for the same user by the same RCASP. A transaction will also be treated as a transfer where the RCASP is unable to determine, at the time the transaction is undertaken, if the transaction is an exchange (for example, trading one crypto-asset for another).

Transfers may include situations where the RCASP facilitates an individual or entity receiving a relevant crypto-asset by means of an airdrop during a hard fork event[29]. In these cases, users receive new crypto-assets along with the ones they already have, and this is called an inbound transfer for the person receiving the new assets.

2.4 Reportable user

2.4.1 “Crypto-asset user”

Under CARF, a crypto-asset user means an individual or entity that is a customer of an RCASP for the purpose of carrying out relevant transactions. Where someone else, other than a Financial Institution or an RCASP, is acting on behalf of that individual or entity, for example as an agent, custodian, nominee, signatory, investment advisor or intermediary, then they are not considered the crypto-asset user. Instead, the original individual or entity is seen as the crypto-asset user.

Where an RCASP provides a service to a merchant that involves carrying out reportable retail payment transactions for or on behalf of that merchant, the RCASP shall treat the merchant’s customer and the merchant as the crypto-asset users in respect of those transactions.

DAC8 follows the CARF definition of “crypto-asset user”, substituting the term “reportable transactions” for “relevant transactions”.

[29] A hard fork event is a change in programming that is incompatible with the old programming. This essentially creates a new blockchain, and sometimes a new cryptocurrency. An airdrop occurs when a new cryptocurrency token is deposited directly into users' wallets.

2.4.2 "Reportable user"

Under CARF, a reportable user means a crypto-asset user that is resident in a reportable jurisdiction and is not an excluded person.

A "reportable jurisdiction"[30] is a jurisdiction with which Ireland has an agreement in place to provide for the automatic exchange of information under the CARF framework.

A list of "reportable jurisdictions" with whom Ireland has an agreement in place is available on the Revenue website[31]. RCASPs are obliged to report in respect of Irish residents, residents of other Member States and residents of reportable jurisdictions.

DAC8 defines a reportable user as a crypto-asset user that is resident in a Member State or other reportable jurisdiction and is not an excluded person.

An entity such as a partnership, limited liability partnership or similar legal arrangement that has no residence for tax purposes shall be treated as resident in the jurisdiction in which its place of effective management is situated.

An "excluded person" means:

(a) an Entity the stock of which is regularly traded on one or more established security markets;
(b) any Entity that is a related entity of an entity described in point (a);
(c) a Governmental entity;
(d) an International organisation;
(e) a Central Bank; or
(f) a Financial Institution other than an investment entity.

An "excluded person" is not treated as a reportable user for the purposes of CARF or DAC8.

2.4.3 Categories of crypto-asset users

Categories of crypto-asset users are classified, firstly, depending on whether they are an individual or an entity and secondly, depending on the date they established a relationship as a customer of an RCASP[32]:

[30] Section IV (D)(9) of Part 1 (2. Rules) of the CARF provides as follows: The term "Reportable Jurisdiction" means any jurisdiction (a) with which an agreement or arrangement is in effect pursuant to which [Jurisdiction] is obligated to provide the information specified in Section II with respect to Reportable Persons resident in such jurisdiction, and (b) which is identified as such in a list published by [Jurisdiction].

[31] List of Reportable Jurisdictions for CARF and DAC8 purposes

[32] Section IV (D) of Part I (2. Rules) of the CARF

a. "Individual Crypto-Asset User" means a crypto-asset user who is an individual.
b. "Pre-existing Individual Crypto-Asset User" means an Individual crypto-asset user that has established a relationship as a customer of the RCASP as of 31 December 2025.
c. "Entity Crypto-Asset User" means a crypto-asset user that is an entity.
d. "Pre-existing Entity Crypto-Asset User" means an entity crypto-asset user that has established a relationship as a customer of the RCASP as of 31 December 2025.

2.4.4 "Controlling persons"

Where a crypto-asset user is an entity, CARF and DAC8 require the RCASP to determine whether the entity is an active entity[33] or a passive entity. Where the entity is a passive entity, the RCASP must identify the controlling persons of that entity.

Controlling persons[34] means the natural persons who exercise control over an entity. Under CARF, controlling persons are to be interpreted in line with the 2012 Financial Action Task Force (FATF) Recommendations, as updated in June 2019 pertaining to virtual asset service providers[35].

Under DAC8, controlling persons are to be interpreted in line with the term of "beneficial owner" as defined in Article 3, point (6) of the AML Directive (4th AMLD)[36] as far as the RCASP is concerned.

Where one or more controlling persons of a passive entity are resident in a reportable jurisdiction or Member State, those controlling persons are treated as reportable users.

[33] Defined in Section IV (D)(11) of Part I (2. Rules) of the CARF

[34] Defined in Section (D)(10) of Part I (2. Rules) of the CARF

[35] FATF (2012 – 2025), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France

[36] Article 3, point (6), of Directive (EU) 2015/849

3 CARF reporting rules - Examples

The following examples illustrate how the CARF reporting rules apply in practice. These examples are based on the CARF commentary and are intended to assist in understanding the scope and operation of the rules.

3.1 Transactions involving relevant crypto-assets

Example 1: Derivative purchase using stablecoins

Crypto-Derivative A is a financial product that allows a user to gain exposure to a crypto-asset by amplifying the potential gains or losses.

User 1 purchases one unit of Crypto-Derivative A using stablecoins through an RCASP.

The RCASP must report the following transactions:

Disposal of stablecoin by User 1:

a. the fiat value at the time of the transaction, and
b. the number of stablecoins sold.

Purchase of Crypto-Derivative A:

a. the fiat value at the time of the transaction, and
b. the number of units purchased.

Example 2: Derivative redemption

User 1 redeems Crypto-Derivative A with the issuer and receives stablecoins.

The RCASP is required to report the following transactions:

Sale of Crypto-Derivate A:

a. the fiat value of Crypto-Derivative A, and
b. the number of units disposed of.

Acquisition of stablecoins:

a. the fiat value of stablecoins, and
b. the number of units received.

Example 3: Futures contract

A buyer and seller enter into a futures contract where the buyer agrees to buy crypto-asset B from the seller on a certain future date.

When the date arrives, the buyer will buy crypto-asset B from the seller at a set price, paid for in fiat currency. The seller must then deliver crypto-asset B to the buyer's digital wallet.

The RCASP is required to report the following transactions:

Disposal of relevant crypto-asset B by the seller:

a. the fiat value of relevant crypto-asset B, and
b. the number of units sold.

Purchase of relevant crypto-asset B:

a. the fiat value of relevant crypto-asset, and
b. the number of units purchased.

3.2 Reportable Retail Payment Transactions

Example 4:

An RCASP facilitates a payment by a customer to a merchant using crypto-assets.

Where the value of the transaction exceeds USD50,000 (or the equivalent amount in another currency):

- the transaction is a reportable retail payment transaction,
- the customer is treated as the crypto-asset user, and
- the RCASP must report the transaction.

The RCASP, when treating the customer who made the payment as a crypto-asset user, should carry out its due diligence procedures to verify the identity of the customer following relevant domestic anti-money laundering rules.

3.3 Agent

Example 5:

An individual grants authority to another person to act on their behalf in transactions with an RCASP.

Where the RCASP has information indicating that the person is acting as an agent:

- The underlying individual is treated as the crypto-asset user, and
- The intermediary is not treated as the reportable user.

3.4 RCASP using another RCASP

Example 6:

RCASP A uses the services of RCASP B to carry out relevant transactions on RCASP B's exchange platform.

RCASP A is treated as a crypto-asset user of RCASP B.

RCASP B is obliged to report the relevant transactions made by RCASP A.

3.5 Transfer where consideration is unknown

Example 7:

A user transfers crypto-assets to another wallet and the RCASP does not know whether consideration was given.

The RCASP must treat the transaction as a transfer and report it accordingly.

3.6 Crypto-asset valuation

Example 8:

An RCASP maintains a trading platform and facilitates a transaction where no direct fiat currency is available.

The RCASP must determine the fair market value using a reasonable and consistently applied methodology, such as:

a. trading prices on its own platform,

b. third party pricing sources,

c. recent valuations, or

d. a reasonable estimation.

4 RCASP registration requirements

An RCASP must register with Revenue before 31 December in the year in which they become an RCASP. The registration portal is currently in development and will launch before the end of 2026.[37]

4.1 Crypto-asset service providers – CARF

For the purposes of CARF, an RCASP is required to determine the jurisdiction in which it is required to register and carry out its CARF due diligence and reporting obligations.

An RCASP may have nexus to more than one jurisdiction. As outlined in section 4.1.1, the CARF has introduced Nexus rules[38] for entities and individuals, which set out rules to be followed by the RCASP in order for the RCASP to determine the jurisdiction it is required to register and report for CARF purposes.

4.1.1 CARF Nexus Hierarchy

For entities, the CARF nexus hierarchy applies in the following order:

- jurisdiction of tax residence,
- jurisdiction of incorporation or organisation, where the entity has legal personality or the obligation to file taxes,
- jurisdiction of place of management, and
- jurisdiction where the entity has a regular place of business, including through a branch.

For individuals, the relevant nexus tests are:

- jurisdiction of tax residence, and
- jurisdiction where the individual has a regular place of business.

An RCASP that has nexus to Ireland under the CARF rules is generally required to register with Revenue unless relief from duplicate registration applies, as outlined in section 8.7.

Under the CARF, the RCASP is required to register in the jurisdiction in which the highest CARF nexus hierarchy applies.

[37] CARF/DAC8 XML Schema – User Guide for Tax Administrations – July 2025

[38] Section I of Part I (2. Rules) of the CARF provides more comprehensive guidance on the CARF registration requirements.

4.2 Crypto-asset service providers – DAC8

Crypto-asset service providers authorised and regulated by:

1. Article 60 of MiCAR (certain financial entities providing crypto-asset services), or
2. Article 63 of MiCAR,

who carry out reportable transactions, must register with Revenue.

Crypto-asset service providers authorised by MiCAR can provide their services in other EU Member States through passporting once they have received their authorisation in a Member State. For these purposes, the European Securities and Markets Authority (ESMA) hold a register of authorised crypto-asset service providers[39].

4.3 Crypto-asset operators – DAC8

For DAC8 purposes, crypto-asset operators who are actively involved in the creation, promotion or distribution of crypto-assets and do not fall under the scope of MiCAR, fall within the definition of an RCASP.

A crypto-asset operator is required to register where it has a sufficient nexus as outlined in Section 2.2.3 above.

The crypto-asset operator must register[40] with Revenue for the purposes of DAC8 by 31 December in the year it first becomes an RCASP.

Once the crypto-asset operator has registered, Revenue will issue a crypto-asset operator ID to the crypto-asset operator.

4.3.1 Crypto-asset operator registration requirements

Each crypto-asset operator must provide the following information when registering with Revenue:

a. name of the crypto-asset operator;

b. postal address of the crypto-asset operator;

c. electronic addresses, including websites of the crypto-asset operator;

d. any TIN[41] [Tax Identification Number] issued to the crypto-asset operator;

[39] Pont 17 of the introduction to Council Directive (EU) 2023/2226 (DAC8)

[40] The registration portal is currently in development and will launch before the end of 2026.

[41] TIN means Taxpayer identification number (or functional equivalent in the absence of a taxpayer identification number). The TIN is any number or code that a competent authority uses to identify a taxpayer.

e. Member State(s) in which reportable users of the crypto-asset operator are resident;

f. any Qualified Non-Union jurisdiction[42] in which the crypto-asset operator carries out due diligence and makes a return.

Where any of the above information changes, the crypto-asset operator must notify the change to Revenue before the last day of the month following the month in which the change occurred.

4.3.2 Crypto-asset operator registered in a different Member State

Where a crypto-asset operator meets the conditions to register in Ireland and also meets the conditions in another EU Member State, then that crypto-asset operator need not register with Revenue provided the crypto-asset operator has:

a. registered as a crypto-asset operator in another Member State for the purposes of DAC8, and

b. received the equivalent of a crypto-asset operator ID from that Member State and this ID has not been revoked.

4.4 Revoking of registration ID

Where a crypto-asset operator is registered with Revenue for the purposes of DAC8 and that crypto-asset operator no longer complies with their obligations under DAC8, then Revenue will revoke their crypto-asset operator ID.

Revenue will not cancel the crypto-asset operators ID until:

a. 2 reminders in writing have issued to the crypto-asset operator advising them of their obligations under DAC8, and

b. a period of 30 days has passed from the date of issuance of the second reminder.

Where Revenue cancels a crypto-asset operator’s ID or if another country cancels a similar ID, then the crypto-asset operator cannot register again with Revenue until it can be shown that:

a. all overdue returns and obligations have been complied with in Ireland, and

b. written assurance has been provided that the crypto-asset operator will comply with the obligation imposed by DAC8.

If the ID was revoked by another Member State, then it must be shown that all overdue returns and obligations have been complied with in that other Member State.

[42] “Qualified Non-Union Jurisdiction” means a Non-Union Jurisdiction that has in effect an Effective Qualifying Competent Authority Agreement with the competent authorities of all Member States which are identified as reportable jurisdictions in a list published by the Non-Union Jurisdiction.

5 RCASPs information collection obligations

RCASPs are required to collect information necessary to identify reportable users and controlling persons and to comply with due diligence and reporting obligations.

A crypto-asset user is obliged to supply the RCASP with all the necessary information required by the RCASP in order for the RCASP to comply with its due diligence and reporting obligations under:

- section 891HA TCA 1997 and CARF, and
- section 891M TCA 1997 and DAC8.

5.1 Self-certification[43]

RCASPs must obtain self-certifications from their users to determine their tax residency and reportable status.

5.1.1 Individual crypto-asset users

A self-certification provided by an individual crypto-asset user is valid if:

i. it is signed by the individual crypto-asset user;
ii. it contains the following information for the individual crypto-asset user:
    a. first and last name;
    b. residence address;
    c. jurisdiction or Member State(s) of residence for tax purposes;
    d. the TIN[44] of each reportable person in respect of each jurisdiction or Member State;
    e. date of birth, and
iii. it is dated on or before the date it is received by the RCASP.

[43] Section III of Part I (2. Rules) of the CARF & Section III of Annex VI of the DAC.

[44] "TIN" means Taxpayer identification number (or functional equivalent in the absence of a taxpayer identification number). The TIN is any number or code that a competent authority uses to identify a taxpayer.

Example 9: Conflicting self-certification

An RCASP obtains a self-certification from an individual crypto-asset user upon the establishment of their relationship.

The country of residence address contained in the self-certification is different to the country of residence address contained in the documentation collected under AML/KYC or customer due diligence procedures.

Due to the conflicting information, the self-certification is incorrect or unreliable and, as a consequence, fails the reasonableness test. The RCASP must obtain a valid self-certification or a reasonable explanation, including documentation supporting the validity of the original self-certification.

5.1.2 Entity crypto-asset users

A self-certification provided by an entity crypto-asset user is valid if:

i. it is signed by the entity crypto-asset user;
ii. it contains the following information for the entity crypto-asset user:
    a. legal name;
    b. address;
    c. jurisdiction or Member State(s) of residence for tax purposes;
    d. the TIN of each reportable person in respect of each jurisdiction or Member State; and
iii. it is dated on or before the date it is received by the RCASP;

5.1.3 Controlling persons

Where an entity crypto-asset user is not an active entity[45] or an excluded person[46], an RCASP must obtain a self-certification for each controlling person.

A self-certification provided by a controlling person is valid if:

i. it is signed by the controlling person;
ii. it contains the following information for the controlling person:
    a. first and last name;
    b. residence address;
    c. jurisdiction or Member State(s) of residence for tax purposes;
    d. the TIN of each reportable person in respect of each jurisdiction or Member State;
    e. date of birth;

[45] Defined in Section IV(D)(11) of Part I (2. Rules) of the CARF

[46] Defined in Section IV(E)(1) of Part I (2. Rules) of the CARF

f. the role in the entity that makes them a controlling person; and

iii. it is dated on or before the date it is received by the RCASP.

5.1.4 Excluded persons

RCASPs are not required to collect the information outlined in sections 5.1.1, 5.1.2 and 5.1.3 for excluded persons.

An RCASP may rely on information in its possession or that is publicly available to ascertain the status of users who fall into the category of excluded persons (refer to section 2.4.2).

Alternatively, an RCASP may obtain a declaration from those users stating they fall into the category of excluded persons. An RCASP can only rely on a declaration when they have no reason to believe or evidence that the declaration is incorrect.

6 Determining whether a crypto-asset user is a reportable user[47]

6.1 Individuals

An RCASP must obtain a self-certification from –

i. an individual crypto-asset user when they begin to use the services of an RCASP, or
ii. an existing individual crypto-asset user by 31 December 2026.

The self-certification should be used by the RCASP to –

i. determine the individual crypto-asset user's residence for tax purposes, and
ii. confirm the reasonableness of such self-certification based on the information obtained by the RCASP, including any documentation collected under AML/KYC or customer due diligence procedures.

If the self-certification shows that the individual crypto-asset user is resident in a reportable jurisdiction or Member State, the RCASP shall treat the individual crypto-asset user as a reportable user.

6.2 Entities

An RCASP must obtain a self-certification from –

i. an entity crypto-asset user when they begin to use the services of an RCASP, or
ii. an existing entity crypto-asset user by 31 December 2026.

The self-certification should be used by the RCASP to –

i. determine the entity crypto-asset user's residence for tax purposes, and
ii. confirm the reasonableness of such self-certification based on the information obtained by the RCASP, including any documentation collected for AML/KYC or customer due diligence procedures.

[47] Section III of Part I (2. Rules) of the CARF & Section III of Annex VI of the DAC.

If the entity crypto-asset user certifies that it has no residence for tax purposes, the RCASP may rely on the place of effective management or the address of the principal office to determine the residence of the entity crypto-asset user.

If the self-certification shows that the entity crypto-asset user is resident in a reportable jurisdiction or Member State, the RCASP shall treat the entity crypto-asset user as a reportable user, unless it reasonably determines based on the self-certification or on information in its possession or on information that is publicly available, that the entity crypto-asset user is an excluded person.

6.3 Entities with controlling persons

An RCASP must obtain a self-certification from an entity crypto-asset user or a controlling person that allows the RCASP to –

i. determine the controlling person's residence for tax purposes, and
ii. confirm the reasonableness of such self-certification based on the information obtained by the RCASP, including any documentation collected for AML/KYC or customer due diligence procedures.

An RCASP is required to use information collected and maintained under its AML/KYC procedures or customer due diligence procedures, provided that such procedures are consistent with the 2012 FATF recommendations[48] or the AML Directive[49], to determine the controlling person of an entity crypto-asset user.

If the RCASP is not legally required to apply procedures consistent with the 2012 FATF recommendations or the AML Directive, it shall apply substantially similar procedures for the purpose of determining the controlling persons.

[48] FATF (2012 – 2025), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France

[49] "Customer Due Diligence Procedures" mean the customer due diligence procedures of an RCASP pursuant to Directive (EU) 2015/849 or similar anti-money laundering requirements to which the RCASP is subject. These procedures include identifying and verifying the identity of the customer (including the beneficial owners of the customer), understanding the nature and purpose of the transactions, and on-going monitoring.

7 Due diligence[50]

The due diligence requirements will allow an RCASP determine the identity and residence of their individual and entity crypto-asset users and also the identity and residence of the natural persons controlling certain entity crypto-asset users.

A crypto-asset user is treated as a reportable user beginning on the date it is identified as such following the due diligence procedures described in this section.

7.1 Verification of crypto-asset user information

An RCASP is required to determine the reasonableness of the information collected under section 5.1 by obtaining a self-certification from a crypto-asset user and by using all information and documents available to the RCASP in its own records.

7.2 Incorrect self-certification

Where an RCASP has reason to believe that any self-certification information collected from an individual crypto-asset user, entity crypto-asset user or controlling person is incorrect or unreliable, the RCASP cannot rely on that self-certification and should obtain a valid self-certification or a reasonable explanation, including documentation supporting the validity of the original self-certification.

7.3 Financial Institutions acting as an RCASP

An RCASP that is also a Financial Institution may rely on due diligence procedures carried out in accordance with sections 2-7 of the Common Reporting Standard[51] or section 2 and section 3 of Annex 1 of Directive (EU) 2023/2226[52].

7.4 Use of existing self-certification

An RCASP may rely on self-certification already collected for other tax purposes, provided that such self-certification satisfies the conditions outlined in subsections 5.1.1, 5.1.2 and 5.1.3.

[50] Section III of Part I (2. Rules) of the CARF

[51] OECD (2025), Consolidated text of the Common Reporting Standard: Standard for Automatic Exchange of Financial Account Information in Tax Matters

[52] “Determining the Controlling Persons of an Account Holder. For the purpose of determining the Controlling Persons of an Account Holder, a Reporting Financial Institution may rely on information collected and maintained pursuant to AML/KYC Procedures, provided that such procedures are consistent with the Directive (EU) 2015/849. If the Reporting Financial Institution is not legally required to apply AML/KYC Procedures that are consistent with the Directive (EU) 2015/849, it shall apply substantially similar procedures for the purpose of determining the Controlling Persons.”

7.5 Third parties fulfilling the collection of information and due diligence obligations

An RCASP may rely on a third party to fulfil the collection of information and due diligence obligations. However, the responsibility for the completion of those requirements remains with the RCASP. In the context of data protection, where a third-party is carrying out these obligations for an RCASP, they should be acting as a data processor and not a joint controller of the data. In addition, all GDPR requirements must be adhered to.

7.6 Retention of documentation

An RCASP is required to maintain all documentation and data that needs to be reported for 6 years.

8 RCASP information reporting obligations[53]

An RCASP must file a return with Revenue by 31 May each year. The return filed relates to the previous calendar year. This section sets out the information that an RCASP is required to include in their return.

An RCASP is also obliged to supply each reportable user with a copy of the information, in respect of that reportable user, that is contained in the return made to Revenue.

8.1 RCASP information

With respect to information relating to the RCASP itself, each RCASP must return the following information –

a. name;
b. postal address;
c. electronic address, including website addresses;
d. TIN issued to that RCASP, including the Member State of issuance of the TIN;
e. where the RCASP is a crypto-asset operator, the crypto-asset operator ID;
f. global legal entity identifier (LEI), or other identifying number, where available.

8.2 Individual reportable user information

With respect to an individual crypto-asset user that is a reportable user, an RCASP must return the following information –

a. name;
b. address;
c. jurisdiction or Member State of residence;
d. TIN;
e. date of birth;
f. place of birth, where it is required under the domestic law of the jurisdiction or Member State in which the individual is resident.

8.3 Entity reportable user information

With respect to an entity crypto-asset user that is a reportable user, an RCASP must return the following information –

a. name;
b. address;
c. jurisdiction or Member State of residence;
d. TIN.

[53] Section II of Part I (2. Rules) of the CARF

8.4 Controlling persons information

With respect to an entity that has one or more controlling persons, an RCASP must return the following information for each controlling person –

a. name;
b. address;
c. jurisdiction or Member State of residence;
d. TIN;
e. date of birth;
f. place of birth, where it is required under the domestic law of the jurisdiction or Member State in which the individual is resident;
g. the role in the entity that makes them a controlling person.

8.5 Information to be reported in respect of relevant/reportable transactions

For each reportable user and each controlling person, an RCASP is required to report the following information for each type of relevant crypto-asset in respect of which it has carried out relevant transactions during the reporting period[54] –

a. the full name of the relevant crypto-asset.

b. in respect of acquisitions against fiat currency –

    i. the aggregate gross amount paid,
    ii. the aggregate number of units, and
    iii. the number of relevant transactions.

There may be instances where a reportable user acquires or disposes a relevant crypto-asset against fiat currency and the RCASP does not have actual knowledge of the underlying fiat currency consideration. This would, for example, be the case if the RCASP only carried out the transfer of the crypto-assets to and from the reportable user, without actual knowledge of the fiat currency leg of the transaction. Such transactions should be reported as set out in (g) and (h) as transfers sent to or by a reportable user.

c. in respect of disposals against fiat currency –

    i. the aggregate gross amount received,
    ii. the aggregate number of units, and
    iii. the number of relevant transactions.

[54] A ”reportable period” is a calendar year. The first reportable period being the calendar year 2026.

For transactions involving (b) and (c), the amounts must be reported in the currency in which they were paid or received. Where the amounts are denominated in different currencies, they must be reported in one currency, converted at the time of each relevant transaction using a consistent conversion method. The reported transactions should identify the currency in which each transaction is being reported.

d. in respect of acquisitions against other reportable crypto-assets –
   i. the aggregate fair market value,
   ii. the aggregate number of units, and
   iii. the number of relevant transactions.

e. in respect of disposals against other reportable crypto-assets –
   i. the aggregate fair market value,
   ii. the aggregate number of units, and
   iii. the number of relevant transactions.

Sometimes, a difficult-to-value relevant crypto-asset is exchanged for a relevant crypto-asset that can be readily valued. In these cases, the RCASP should use the value of the easier-to-value crypto-asset to establish a currency value for the difficult-to-value relevant crypto-asset.

f. in respect of reportable retail payment transactions –
   i. the aggregate fair market value,
   ii. the aggregate number of units, and
   iii. the number of reportable retail payment transactions.

For reportable retail payments transactions, the customer of the merchant must also be treated as a crypto-asset user (subject to the conditions specified in the definition of crypto-asset user). This means that both the merchant and the merchant's customer may be reportable users in respect of the transaction.

g. in respect of transfers to reportable users that are not covered by (b) and (d)-
   i. the aggregate fair market value,
   ii. the aggregate number of units, and
   iii. the number of relevant transactions, subdivided by transfer type where known by the RCASP.

h. in respect of transfers by reportable users that are not covered by (c), (e) and (f) –
   i. the aggregate fair market value,
   ii. the aggregate number of units, and
   iii. the number of relevant transactions, subdivided by transfer type where known by the RCASP.

Where an RCASP knows that transfers carried out for a reportable user are due to an airdrop[55] (resulting from a hard-fork), an airdrop (for reasons other than a hard-fork), income derived from staking, the disbursement, reimbursement or associated return on a loan, or an exchange for goods or services, it should indicate the aggregate fair market value, aggregate number of units and number of transfers effectuated for each transfer type.

i. in respect of transfers to wallet addresses or distributed ledger addresses that are not known to be associated with a virtual asset service provider or financial institution –
    i. the aggregate fair market value, and
    ii. the aggregate number of units.

For transactions falling under (d) to (i) inclusive, the amounts must be reported in the currency in which they were paid or received.

However, where the amounts were paid or received in different types of currencies, they must be reported in a single currency, converted at the time of each relevant transaction, using the same conversion method every time. The reported transactions should show in which currency each transaction is being reported.

Transfers under (g), (h) and (i) include acquisitions and disposals in respect of which the RCASP has no actual knowledge of the consideration paid or received, as well as transfers that are not acquisitions or disposals (e.g. a transfer of crypto-assets by a user to its private wallet or to its account with another RCASP).

For all reporting categories, the rules require the adding up of all transactions attributable to each reporting category for each type of relevant crypto-asset. For example, if units of a relevant crypto-asset can be mutually substituted for corresponding units of the same relevant crypto-asset, then they should all be treated as the same type of relevant crypto-asset for aggregation purposes. If, however, a relevant crypto-asset is non-fungible, and different variations of the relevant crypto-asset do not have the same value among fixed units, each unit should be treated as a separate type of relevant crypto-asset.

[55] An airdrop is the distribution of crypto-assets to wallet addresses, usually without payment, either as a promotional activity or as part of a network event.

8.6 Where an RCASP is required to report – CARF

An RCASP may be subject to CARF reporting and due diligence obligations in more than one jurisdiction. For CARF purposes, reporting and due diligence are determined by applying the CARF nexus hierarchy to identify the jurisdiction with the highest applicable nexus.

For entities, the CARF nexus hierarchy applies in the following order:

- jurisdiction of tax residence,
- jurisdiction of incorporation or organisation, where the entity has legal personality or the obligation to file taxes,
- jurisdiction of place of management, and
- jurisdiction where the entity has a regular place of business, including through a branch.

For individuals, the relevant nexus tests are:

- jurisdiction of tax residence, and
- jurisdiction where the individual has a regular place of business.

An RCASP should complete its CARF due diligence and reporting obligations in the jurisdiction with the highest applicable CARF nexus.

8.7 Duplicate Reporting – CARF

For CARF purposes, where more than one nexus applies to an RCASP, duplicate reporting is prevented by the RCASP completing all due diligence and reporting in one jurisdiction, determined by applying the CARF nexus hierarchy.

An RCASP should determine the jurisdiction with the highest applicable CARF nexus and complete its CARF reporting and due diligence obligations in that jurisdiction.

Where an RCASP has an equal level of CARF nexus in more than one jurisdiction, the RCASP may avoid duplicate reporting by confirming[56] to Revenue that the reporting and due diligence procedures have been carried out in one of those jurisdictions.

[56] Section I(H) of Part 1 (2. Rules) of the CARF

Example: 10

CryptoCoin Limited is an entity RCASP that is tax resident in Ireland and is incorporated in the United Kingdom. CryptoCoin Limited therefore has two nexuses and would potentially be subject to duplicative reporting for CARF purposes.

The highest nexus for CARF is tax residency.

CryptoCoin Limited will be subject to reporting and due diligence in Ireland and will complete the reporting and due diligence in Ireland for all transactions it effectuates.

8.8 Branch reporting - CARF

Branches are within the scope of CARF in accordance with Section I(B) of the CARF.

Where an RCASP is:

a. subject to the reporting and due diligence obligations in a jurisdiction where it has a branch for CARF purposes, and

b. does not otherwise have a higher nexus in a jurisdiction implementing CARF,

the branch of the RCASP will be responsible for the reporting of all transactions effectuated by the RCASP and not just the transactions of the branch.

As reportable jurisdictions are implementing CARF on a staggered basis, transitional relief will apply to the reporting responsibilities of the Irish branch in the initial reporting periods of 2027, 2028 and 2029, where the RCASP's head office is located in a jurisdiction that is committed to implementing CARF in 2027, 2028 or 2029. During the transitional period, branches will generally only be required to report transactions carried out through the branch.

A list of jurisdictions that have committed to implementing CARF is maintained by the OECD[57].

8.9 Where an RCASP is required to report – DAC8

An RCASP that carries out reportable transactions is required to comply with the DAC8 due diligence and reporting obligations in Ireland where it has an Irish nexus, including where it is:

[57] Jurisdictions committed to implement the Crypto-Asset Reporting Framework.

i. regulated or allowed to provide crypto-asset services under Article 60 or Article 63 of MiCAR,
ii. an entity or individual resident in Ireland for tax purposes, or
iii. an entity incorporated in Ireland and either has legal personality or is obliged to file tax returns or tax information returns regarding their income, or
iv. an entity that has a place of management in Ireland, or
v. an entity or individual that has a regular place of business in Ireland.

In addition, an RCASP that carries out reportable transactions through a branch in Ireland is required to comply with the DAC8 due diligence and reporting obligations in Ireland.

An RCASP that falls within one of the above categories is required to report in Ireland unless relief applies under subsections 8.10 and 8.11.

8.10 Order of reporting priority and relief from duplicate reporting - DAC8

An RCASP may have nexus to more than one jurisdiction for DAC8 purposes. Where this occurs, DAC8 applies a hierarchy of nexus rules to determine which jurisdiction has primary reporting and due diligence responsibility.

For entities, the reporting obligations should be fulfilled in the following order of priority:

i. jurisdiction in which the RCASP is regulated or allowed to provide crypto-asset services under Article 60 or Article 63 of MiCAR;
ii. jurisdiction of tax residence;
iii. jurisdiction of incorporation[58];
iv. jurisdiction of place of management;
v. jurisdiction of regular place of business.

For individuals, the relevant nexus tests are:

i. jurisdiction of tax residence;
ii. jurisdiction of regular place of business.

Where an RCASP is regulated or allowed to provide crypto-asset services under Article 60 or Article 63 of MiCAR, Ireland will generally be the highest priority reporting jurisdiction for DAC8 purposes.

[58] and either has legal personality or is obliged to file tax returns or tax information returns regarding income.

An RCASP linked to Ireland is not required to carry out the DAC8 due diligence requirements or to make a return in Ireland in respect of Reportable Users or Controlling Persons where –

a. the RCASP carries out the equivalent reporting and due diligence obligations in another Member State or Qualified Non-Union Jurisdiction[59] that has an equal or higher priority nexus, and
b. the RCASP lodges a notification with Revenue confirming that the reporting and due diligence have been completed by the RCASP in that other Member State or Qualified Non-Union Jurisdiction.

Where reporting obligations are fulfilled in an equal or higher priority Member State or Qualified Non-Union Jurisdiction, duplicate reporting in Ireland is not required.

8.11 Branch reporting -DAC8

An RCASP is not required to carry out DAC8 due diligence or reporting obligations in Ireland in relation to reportable transactions carried out through a branch located in another Member State or Qualified Non-Union Jurisdiction where:

a. the branch carries out the reporting and due diligence obligations in that jurisdiction, and
b. the RCASP retains evidence demonstrating that those obligations have been fulfilled by the branch.

8.12 Procedures to follow when a reportable user or a controlling person has not provided the necessary information

Where an RCASP has requested the necessary information to meet their CARF or DAC8 obligations from a reportable user or a controlling person and they fail to provide the requested information, then the RCASP must issue two reminders, in writing, to the reportable user or to the controlling person requesting the necessary information.

If 60 days have passed from the date of issuance of the second reminder and the necessary information remains outstanding then the RCASP must –

i. close the account of the reportable user or controlling person, and
ii. prevent the reportable user or controlling person from reopening the account or opening a new account until such a time as the necessary information has been provided.

[59] A "Qualified non-Union Jurisdiction" means a non-Union country that holds qualifying competent authority agreements with the competent authorities of all Member States which are identified as reportable jurisdictions in a list published by the non-Union jurisdiction

9 Penalties

Penalties applicable to RCASPs arise under section 891HA and section 891M TCA 1997.

A penalty of €19,045 is applicable where an RCASP –

(a) fails to make a return of the information set out in section 8, or
(b) makes an incorrect or incomplete return of the information set out in section 8.

In addition, a further penalty of €2,535 is applicable for each day a return remains outstanding under paragraph (a).

A penalty of €1,265 applies to an RCASP who does not comply with the requirements of an authorised officer in the exercise or performance of the officer's powers or duties.

Where an RCASP –

(a) fails to register with Revenue as set out in section 4, or
(b) does not comply with the due diligence procedures as set out in section 5,

that RCASP shall be liable to a penalty of €4,000.

10 Maintaining records

An RCASP is required to keep records of the procedures applied and information relied upon in order to comply with their obligations under section 891HA and section 891M TCA 1997 for a period of 6 years from the end of the year in which the procedures were applied or information was relied upon.

11 Data protection

Where RCASPs are reporting under DAC8, they are considered to be data controllers when, acting alone or jointly, they determine the purposes and means of the processing of personal data within the meaning of Regulation (EU) 2016/679[60]. In this context each RCASP should carry out their own data protection impact assessment and ensure they meet all of their data protection obligations.

[60] Regulation (EU) 2016/679

For example, each RCASP shall -

a. inform each reportable user or controlling person, who is an individual, that information relating to that individual will be collected and transferred, and
b. provide to each reportable user or controlling person that is an individual, all information that the individual is entitled to from the data controller in sufficient time for that individual to exercise his/her data protection rights and, in any case, before the information is reported.