5 Commentary to the Multilateral Competent Authority Agreement

Introduction

1. In order to exchange information under the Crypto-Asset Reporting Framework (CARF), Jurisdictions must have a legal framework in place that allows for the automatic exchange of information with partner Jurisdictions. This legal framework should include both a legal basis for the information exchanges, as well as administrative agreements to determine the scope, timing and method of the information exchanges.

2. Jurisdictions can have a legal basis for tax information exchanges pursuant to the Convention on Mutual Administrative Assistance in Tax Matters (Convention). Pursuant to Article 6 of the Convention, two or more Parties to the Convention can mutually agree to automatically exchange predefined foreseeably relevant information in accordance with the procedures determined by the Parties by mutual agreement. In the context of the Common Reporting Standard, this multilateral approach has proven to be an efficient route to put in place widespread networks of exchange relationships as it allows Jurisdictions to efficiently activate bilateral exchange relationships.

3. To operationalise Article 6 of the Convention, Jurisdictions must also have in place administrative agreements to determine, in particular, the information to be automatically exchanged and the time and method of the exchanges. For the CARF, this Multilateral Competent Authority Agreement (CARF MCAA), which is based on Article 6 of the Convention, sets out the detailed modalities of the exchanges taking place every year on an automatic basis.

4. The CARF MCAA consists of:

- a declaration to be signed by the Competent Authority of the Jurisdiction or its designated representative to become a signatory of the CARF MCAA;
- a preamble which explains the purpose of the CARF MCAA and contains representations on domestic reporting and due diligence rules that underpin the exchange of information pursuant to the CARF MCAA. It also contains representations on confidentiality, data protection safeguards and the existence of the necessary infrastructure;
- eight sections containing the agreed provisions of the CARF MCAA: Section 1 deals with definitions, Section 2 covers the items of information to be exchanged, Section 3 the time and manner of the exchange, Section 4 collaboration on compliance and enforcement and Section 5 the confidentiality and data safeguards that must be respected. Consultations between the Competent Authorities, amendments to the CARF MCAA and the general terms of the CARF MCAA, including the activation of exchange relationships through the submission of notifications, the suspension, deactivation and termination, as well as the role of the Co-ordinating Body Secretariat are dealt with in Sections 6, 7 and 8.

- seven notifications required under Section 7(1) for the CARF MCAA to enter into effect for a Competent Authority.

5. The CARF MCAA is a multilateral agreement based on the principle that automatic exchange is reciprocal and that the exchange will be done on a bilateral basis. There may be instances where Competent Authorities wish to enter into a non-reciprocal bilateral exchange relationship (e.g. where one Jurisdiction does not have an income tax), as confirmed in a notification provided pursuant to Section 7(1)(b).

6. As an alternative to the CARF MCAA, Jurisdictions can also establish automatic exchange relationships through bilateral competent authority agreements based on bilateral double tax treaties or tax information exchange agreements that permit the automatic exchange of information, or the Convention on Mutual Administrative Assistance in Tax Matters. Jurisdictions could also enter into a self-standing intergovernmental agreement or rely on regional legislation covering both the reporting obligations and due diligence procedures coupled with the exchange of information modalities.

Commentary on the Declaration

1. To become a signatory of the CARF MCAA, the Competent Authority of the Jurisdiction or its designated representative must sign the Declaration and provide it, together with the text of the CARF MCAA, to the Coordinating Body Secretariat.

2. The CARF MCAA will only enter into effect with respect to another Competent Authority once both Competent Authorities have signed the Declaration, have submitted all associated notifications pursuant to Section 7(1) to the Coordinating Body Secretariat and have included each other on the list of intended exchange partners in the notification provided pursuant to subparagraph 1g) of Section 7.

Commentary on the Preamble

1. The preamble ("whereas clauses") provides relevant context, explains the purpose of the CARF MCAA and contains representations of the signatories.

2. The first clause contains a confirmation that the Jurisdictions of the signatories to the CARF MCAA are Parties to, or territories covered by the Convention, which is a condition for being able to sign the CARF MCAA.

3. The second and third clauses serve as an introduction and clarify that the purpose of the CARF MCAA is to tackle tax avoidance and evasion and to improve tax compliance.

4. The fourth clause sets out the representations by the Competent Authorities that the laws of their respective Jurisdictions require, or are expected to require, Reporting Crypto-Asset Service Providers to report information regarding Relevant Crypto-Assets, consistent with the scope of exchange contemplated by Section 2. The language used in the fourth clause allows Competent Authorities, that so wish, to sign the CARF MCAA before their Jurisdiction has the relevant rules on due diligence and reporting in place.

5. The fifth clause provides that future amendments to the Crypto-Asset Reporting Framework are expected to be reflected in the domestic legislation of the Jurisdictions and that once enacted by a Jurisdiction, any reference to the term Crypto-Asset Reporting Framework would be deemed to refer to the amended version in respect of that Jurisdiction.

6. The sixth clause sets out the legal basis that authorises the automatic exchange of information and allows the Competent Authorities to agree the procedures to be applied to such automatic exchanges. The scope agreed to is consistent with the scope of exchange contemplated by Section 2.

7. The seventh clause specifies that, whereas the Convention allows for two or more Parties to mutually agree to exchanging specified information automatically, the actual exchange of information would occur on a bilateral basis (i.e. from the sending Competent Authority to the receiving Competent Authority).

8. The eighth clause sets out the representations by the Competent Authorities that their Jurisdictions have in place (i) appropriate safeguards to ensure the confidentiality of the information received and (ii) an infrastructure that allows for an effective exchange relationship.

9. The ninth clause restates the purpose of the CARF MCAA to improve international tax compliance with respect to Relevant Crypto-Assets. It also clarifies that the application of the CARF MCAA may depend on the successful completion of national legislative procedures (e.g. Parliamentary approval and/or a referendum) and reiterates that the conclusion of the CARF MCAA is subject to the Parties' adherence to the confidentiality, data safeguards and other protections, including that the use of the information exchanged is limited to the extent prescribed under the Convention.

Commentary on Section 1 concerning definitions

Paragraph 1 – Definitions

1. Subparagraph 1a) defines the Jurisdictions of the Competent Authorities that have signed the CARF MCAA and refers to a country or a territory in respect of which the Convention is in force (original Convention) or in effect (in case of the amended Convention) either through ratification or territorial extension.

2. The definition of the term "Competent Authority" contained in subparagraph 1b) refers to the persons and authorities listed in Annex B of the Convention.

3. The definition of the term "Crypto-Asset Reporting Framework" in subparagraph 1c) refers to the international framework for the automatic exchange of information with respect to Crypto-Assets (which includes the Commentaries) developed by the OECD, with G20 countries.

4. It is possible that the CARF, including the IT modalities such as the XML schema, will be updated from time to time as more Jurisdictions implement, and obtain experience with, the CARF. Furthermore, in the context of the CARF MCAA, Competent Authorities may sign on different dates and because of the differing dates of signature the CARF may have been updated in the interim. In this respect, and to ensure that there is an understanding that all Jurisdictions would be expected to implement the most recent version of the CARF with respect to the Reporting Crypto-Asset Service Providers that are subject to due diligence and reporting requirements in their Jurisdiction, the fifth whereas-clause states that it is "expected that the laws of the Jurisdictions would be amended from time to time to reflect updates to the Crypto-Asset Reporting Framework and once such amendments are enacted by a Jurisdiction the definition of the term Crypto-Asset Reporting Framework would be deemed to refer to the updated version in respect of that Jurisdiction".

5. The definition of the term "Co-ordinating Body Secretariat" in subparagraph 1d) refers to the OECD Secretariat that, pursuant to paragraph 3 of Article 24 of the Convention, provides support to the Co-ordinating Body that is composed of representatives of the Competent Authorities of the Parties to the Convention.

6. In accordance with subparagraph 1e), the CARF MCAA is an "Agreement in effect" in respect to any two Competent Authorities, if they have included each other in their list of intended exchange partners (notification pursuant to subparagraph 1g) of Section 7) and have satisfied the other conditions set out in paragraph 2 of Section 7. A list of the Competent Authorities between which the CARF MCAA is in effect will be published on the OECD website.

Paragraph 2 – General rule of interpretation

7. Paragraph 2 sets out the general rule of interpretation. The first sentence of paragraph 2 makes clear that any capitalised terms used in the CARF MCAA but not defined therein are meant to be interpreted consistently with the meaning given to them in the CARF.

8. The second sentence of paragraph 2 provides that, unless the context otherwise requires or the Competent Authorities agree to a common meaning, any term not otherwise defined in the CARF MCAA or in the Crypto-Asset Reporting Framework has the meaning that it has at that time under the law of the Jurisdiction applying the CARF MCAA. In this respect any meaning under the applicable tax laws of that Jurisdiction will prevail over a meaning given to that term under other laws of that Jurisdiction. Further, when looking at the context, the Competent Authorities should consider the Commentary on the Crypto-Asset Reporting Framework.

Commentary on Section 2 concerning Exchange of Information with Respect to Reportable Persons

1. Paragraph 1 provides the legal basis for the exchange and sets out that the information will be exchanged on an annual basis. Information may also be exchanged more frequently than once a year. For example, when a Competent Authority receives corrected data from a Reporting Crypto-Asset Service Provider, that information would generally be sent to the other Competent Authority as soon as possible after it has been received. The information to be exchanged is the information obtained pursuant to Section II of the Crypto-Asset Reporting Framework and is further specified in paragraph 3.

2. Paragraph 1 also makes clear that the exchange of information is subject to the applicable reporting and due diligence rules of the Crypto-Asset Reporting Framework. Thus, where those rules do not require the reporting of, for instance, a TIN or place of birth with respect to a particular Reportable Person, there is also no obligation to exchange such information.

3. Paragraph 2 describes the requirements with respect to Jurisdictions that have indicated they are to be listed as non-reciprocal Jurisdictions on the basis of a notification pursuant to subparagraph 1b) of Section 7. These Jurisdictions will send, but not receive, information specified in paragraph 3. Conversely, Jurisdictions that are not listed as non-reciprocal Jurisdictions will receive the information specified in paragraph 3 from non-reciprocal Jurisdictions, but will not send such information to non-reciprocal Jurisdictions.

4. Paragraph 3 lists the information to be exchanged with respect to each Reportable Person of another Jurisdiction. For all reporting categories under Section 2 (3)(c)(ii) through (3)(c)(ix), the Crypto-Asset Reporting Framework requires the aggregation, i.e. summing up, of all Relevant Transactions attributable to each reporting category for each type of Relevant Crypto-Asset, as converted and valued pursuant to paragraphs D and E of Section II of the Crypto-Asset Reporting Framework and paragraphs 33-41 of the Commentary on Section II.

Commentary on Section 3 concerning Time and Manner of Exchange of Information

Paragraph 1 – Time of exchange of information

1. Paragraph 1 provides that the information under Section 2 must be exchanged within nine months after the calendar year to which the information relates. The first year with respect to which the information is exchanged is the year indicated by the signatory Competent Authority in its notification pursuant to subparagraph 1a) of Section 7, in which it confirms its Jurisdiction has in place the required implementing legislation. The nine-month timeline in paragraph 1 is a minimum standard and Jurisdictions are free to exchange prior to the prescribed timelines.

2. Paragraph 1 also provides that notwithstanding the year that the Competent Authorities have indicated in their notification pursuant to Section 7(1)(a) as the year in respect of which the first exchange will take place, information is only required to be exchanged with respect to a calendar year if both Jurisdictions have in place legislation to give effect to the Crypto-Asset Reporting Framework with respect to such calendar year. A Jurisdiction may, however, choose, subject to its domestic laws, to exchange the information with another Jurisdiction in respect of (earlier) years, if it has given effect to the Crypto-Asset Reporting Framework and has the CARF MCAA in effect with the Competent Authority of such Jurisdiction.

3. The following example illustrates the operation of the last sentence of paragraph 1. Jurisdictions A and B have signed the CARF MCAA. Jurisdiction A provides its notifications pursuant to Section 7(1) on 7 June 2025, indicating that it has legislation in effect that requires reporting with respect to 2026. Jurisdiction B provides its notifications on 1 November 2025, indicating that it has legislation in effect to provide reporting with respect to 2027. In this case the last sentence of paragraph 1 will operate such that Jurisdiction A does not have an obligation to exchange information in respect of 2026. Both Jurisdictions A and B will have an obligation to exchange information with respect to 2027. However, Jurisdiction A may choose, subject to its domestic laws, to send information to Jurisdiction B in respect of 2026 even though Jurisdiction A will not receive information in respect of 2026.

Paragraphs 2 and 3 – Information technology modalities

CARF schema and user guide

4. Paragraph 2 provides that the Competent Authorities will automatically exchange the information described in Section 2 in a common schema in Extensible Markup Language, the CARF XML Schema.

Data transmission including encryption

5. Paragraph 3 provides that the Competent Authorities will transmit the information through the OECD Common Transmission System, which is the commonly developed secure transmission system in use by Competent Authorities across the globe for the transmission of confidential tax information. The information must further be prepared and encrypted in line with the latest internationally-agreed standards.

6. Alternatively, Competent Authorities may use another method for data transmission, as specified by such Competent Authorities in their notification pursuant to subparagraph 1d) of Section 7. Any alternative transmission method should meet equivalent security, encryption and file preparation standards to those applicable to the OECD Common Transmission System in order to ensure the confidentiality and integrity of data throughout the transmission, as to ensure that the data is in no case made available or disclosed to unauthorised persons and is not modified or altered in an unauthorised manner.

7. One method of encryption in common use for exchange of information uses both a public and a private key. Public key cryptography has been in use for some decades and allows parties to exchange

encrypted data without communicating a shared secret key in advance. The sending party encrypts the data file with a public key, and only the receiving party holds the secure private key that allows the data to be decrypted. There are standards for the length of encryption keys in use internationally that are recognised as providing the appropriate level of security for personal financial data, both now and for the foreseeable future, such as advanced encryption standard (AES) 256.

Commentary on Section 4 concerning Collaboration on Compliance and Enforcement

1. Section 4 sets out the expectations in terms of the collaboration between the Competent Authorities on compliance and enforcement. It provides that if one Competent Authority has reason to believe that an error may have led to incorrect or incomplete information reporting or there is non-compliance by a Reporting Crypto-Asset Service Provider that Competent Authority should notify the other Competent Authority. The notified Competent Authority is then expected to take all appropriate measures available under its domestic law to address the errors or non-compliance described in the notice. This includes instances where a Reportable Person invokes data subject rights to have its incorrect data corrected or deleted. Prior to sending a formal notification, Competent Authorities should consider consulting informally on the errors or instances of non-compliance identified. See the Commentary on Section V of the Crypto-Asset Reporting Framework regarding the rules and administrative procedures that Jurisdictions must have in place to ensure that the Crypto-Asset Reporting Framework is effectively implemented.

2. Any notification under this Section must clearly set out the error or non-compliance and the reasons for the belief that such error or non-compliance has occurred. The notified Competent Authority should provide a response or an update as soon as possible and no later than 90 calendar days of having received the notification from the other Competent Authority. If the issue has not been resolved, the notified Competent Authority should provide the other Competent Authority with updates every 90 days. If, however, after reviewing and considering the notification in good faith, the notified Competent Authority does not agree that there is, or has been, an error or non-compliance it should, as soon as possible, advise the other Competent Authority in writing of such determination and explain the reasons for it.

Commentary on Section 5 concerning Confidentiality and Data Safeguards

1. Confidentiality of taxpayer information has always been a fundamental cornerstone of tax systems, as well as for the international exchange of tax information. Jurisdictions have a legal obligation to ensure that information exchanged remains confidential and is used only in accordance with the terms of the agreement under which it was exchanged. In order to have confidence in their tax systems and comply with their obligations under the law, taxpayers need to know that financial information is not disclosed inappropriately, whether intentionally or by accident. Taxpayers and governments will only trust international exchange if the information exchanged is used and disclosed only in accordance with the instrument on the basis of which it was exchanged. This is a matter of both the legal framework, but also of having systems and procedures in place to ensure that the legal framework is respected in practice and that there is no unauthorised disclosure or use of information. The ability to protect the confidentiality of tax information is also the result of a “culture of care” within a tax administration which includes the entire spectrum of systems, procedures and processes to ensure that the legal framework is respected in practice and information security and integrity is also maintained in the handling of information. As the sophistication of a tax administration increases, the confidentiality processes and practices must keep pace to ensure that information exchanged remains confidential and is used appropriately. In this respect, several

Jurisdictions have specific rules on the protection of personal data and data subject rights, which also apply to taxpayer information.

2. Section 5 together with Section 7 and the representations in the eighth whereas-clause of the preamble explicitly recognise the importance of confidentiality and data safeguards in connection with the automatic exchange of information under the CARF MCAA. The Commentary on this Section briefly discusses paragraphs 1 and 2 followed by a comprehensive description of the approach towards confidentiality and data safeguarding in connection with the Crypto-Asset Reporting Framework.

Paragraph 1 – Confidentiality and protection of personal data

3. All information exchanged under the CARF MCAA is subject to the confidentiality rules and other safeguards provided for in the Convention. This includes the limitations based on the purposes for which the information may be used and limits to whom the information may be disclosed. In particular, Article 22 of the Convention states that the information exchanged with a Party should only be disclosed to persons or authorities concerned with the assessment, collection or recovery of, the enforcement or prosecution in respect of, or the determination of appeals in relation to taxes of that Party and that the Party may use the information and only for such purposes.

4. Many Jurisdictions have specific rules on the protection of personal data and data subject rights which apply to taxpayer information. For example, special data protection rules apply to information exchanges by EU Member States (whether the exchange is made to another EU Member State or a third Jurisdiction).[1] These rules include, inter alia, the data subject's right to information, access, correction, redress and the existence of an oversight mechanism to protect the data subject's rights.

5. Paragraph 1 of Article 22 of the amended Convention provides that "any information obtained by a Party […] shall be treated […], to the extent needed to ensure the necessary level of protection of personal data, in accordance with the safeguards which may be specified by the supplying Party as required under its domestic law". In that light, paragraph 1 of Section 5 provides that the supplying Competent Authority may specify such safeguards in a notification provided pursuant to subparagraph 1e) of Section 7. The Competent Authority receiving the information confirms in its notification provided pursuant to subparagraph 1g) of Section 7 (intended exchange partners) that its Jurisdiction is compliant with the requirements specified by Competent Authorities that are selected as intended exchange partners. The Competent Authority receiving the information shall treat the information in compliance not only with its own domestic law, but also with additional safeguards that may be required to ensure data protection under the domestic law of the supplying Competent Authority. Such additional safeguards, as specified by the supplying Competent Authority, may for example relate to individual access to the data, correction, deletion, or the right to redress. The specification of the safeguards may not be necessary if the supplying Competent Authority is satisfied that the receiving Competent Authority ensures the necessary level of data protection with respect to the data being supplied. In any case, these safeguards should be limited to what is needed to ensure the protection of personal data without unduly preventing or delaying the effective exchange of information, in recognition of the significant public interest of the exchange of information in tax matters.

6. Exchange of information instruments, including Article 21 of the Convention, generally provide that information does not have to be supplied to another jurisdiction if the disclosure of the information would be contrary to the *ordre public* (public policy) of the jurisdiction supplying the information. While it is rare for this to apply in the context of information exchanges between Competent Authorities, certain jurisdictions may, for instance, require their Competent Authorities to specify that information they supply may not be used or disclosed in proceedings that could result in the imposition and execution of the death penalty or torture or other severe violations of human rights (such as for example when tax investigations are motivated by political, racial, or religious persecution) if such exchange would contravene the public policy of the supplying jurisdiction.

Paragraph 2 – Breach of confidentiality

7. Ensuring ongoing confidentiality of information received under the applicable legal instrument is critical. Paragraph 2 of Section 5 provides that in the event of any breach of confidentiality or failure of safeguards in the Jurisdiction (including the additional safeguards specified by the supplying Competent Authority) the Competent Authority of such Jurisdiction must immediately notify the Co-ordinating Body Secretariat of such breach or failure, including any sanctions or remedial actions consequently imposed. The content of any such notice must itself respect the confidentiality rules and must be in accordance with the domestic law of the Jurisdiction where the breach or failure occurred. Further, Section 7 explicitly provides that non-compliance with the confidentiality and data safeguard provisions (including the additional safeguards specified by the supplying Competent Authority) would be considered significant non-compliance and a justification for immediate suspension of the CARF MCAA.

Ensuring ongoing compliance with confidentiality and data safeguarding requirements

8. Three building blocks are essential in order to ensure appropriate safeguards are in place to protect the information exchanged automatically: (i) a legal framework that ensures the confidentiality and appropriate use of exchanged information in accordance with international legal instruments; (ii) an information security management (ISM) system that adheres to internationally recognised standards or best practices; and (iii) enforcement provisions and processes to address the occurrence of confidentiality breaches and misuse of information.

Legal framework

9. Jurisdictions' domestic legal framework should include provisions sufficient to protect the confidentiality of taxpayer information, including exchanged information, and provide only for specific and limited circumstances under which such information can be disclosed and used, such circumstances being consistent, in relation to exchanged information, with the terms of the applicable international exchange instrument (bilateral or multilateral) under which the information was exchanged.

Information Security Management (ISM) framework

10. Tax administrations that are authorised to access information exchanged in accordance with paragraph 2 of Article 22 of the Convention or equivalent provisions in other international exchange agreements (hereafter, 'relevant organisations') must have an ISM policy and systems to ensure that information can be used solely for intended purposes and to prevent disclosure to unauthorised persons. An ISM system is a set of governance arrangements, policies, procedures and practices concerned with information security risks, including IT-related risks. ISM systems must adhere to internationally recognised standards or best practices.

11. Internationally recognised standards or best practices refers to the "ISO/IEC 27000-series," published jointly by the International Organisation for Standardisation (ISO) and the International Electro-technical Commission (IEC), which provides best practices on information security management, risks, and controls within the context of an overall ISM system.

12. Relevant organisations must meet the ISM requirements in their overall ISM system, in their implementation of various security controls, and in their operational framework to test the effectiveness of these controls, as follows:

13. In respect of the overall ISM system, relevant organisations should:

- display a clear understanding of the lifecycle of exchanged information within the organisation, and be committed to safeguard its confidentiality and appropriate use;

- manage information security through the medium of a written information security policy that is part of an overarching security framework that clearly defines security roles and responsibilities, is owned by senior management and is kept up to date;
- address information security, including technology, through appropriate operational arrangements and as an integrated part of the management of relevant business processes;
- systematically manage their information security risks, taking account of the threats, vulnerabilities, and impacts; and
- have appropriate arrangements to manage and maintain business continuity.

14. In respect of human resources controls, relevant organisations should:

- ensure that security roles and responsibilities of employees and contractors are defined, documented, and clearly communicated in terms of engagement, and regularly reviewed in accordance with the information security policy (this should include confidentiality and non-disclosure agreements);
- undertake background checks with appropriate vetting of all candidates for employment, employees, and contractors, in accordance with accepted best practices and perceived risks;
- ensure that all employees and contractors receive regular and up to date security training and awareness, with employees and contractors in sensitive roles receiving additional guidance relevant to the handling of more sensitive material;
- ensure that employees apply security policies and procedures; and
- have human resources policies and processes relating to the termination of engagement that protect sensitive information.

15. In respect of physical and logical access controls, relevant organisations should:

- have a physical access control policy owned by senior management;
- adequately protect physical premises and have appropriately defined internal and external secure perimeters;
- have a logical access control policy owned by senior management and based on the ‘need to know’ and ‘least privileged access’ principles; and
- have policies, processes and procedures, owned by senior management and not solely the organisation’s IT function, that govern logical access, and effective processes for the provisioning and auditing of logical access and for the identification and authentication of users.

16. In respect of IT system security, relevant organisations should:

- make security an integral part of providing technology services, have a security plan for applications, and harmonise their systems with security;
- deploy an appropriate range of security controls;
- adequately manage their assets;
- appropriately manage supplier service delivery; and
- assure the continuity of IT services based on service level agreements.

17. In respect of the protection of information, relevant organisations should:

- effectively manage information in accordance with a set of policies and procedures throughout the information management lifecycle (including document naming, classification, handling, storage, monitoring, auditing, and destruction; and including devices and media that hold information); and

- have processes in place for information received from other Competent Authorities to ensure that obligations under international exchange agreements are met, including to prevent comingling with other information.

18. In respect of the operations management framework, including incident management, change management, monitoring and audit, relevant organisations should:

- be aware of the controls that protect exchanged information and have appropriate plans in place to manage them;
- have appropriate monitoring and logging arrangements in place, including to detect unauthorised access, use or disclosure of information;
- analyse and act upon security risks;
- have processes and procedures for the identification and management of known vulnerabilities;
- have a change management process, with security integrated into it;
- have an incident management system that covers all types of security incidents; and
- have internal audit and external audit functions.

Enforcement provisions and processes to address confidentiality breaches

19. Jurisdictions must further have penalties and/or sanctions for non-compliance with the required confidentiality and data safeguards in their legal framework to ensure compliance. The legal and ISM frameworks must be reinforced by adequate administrative rules, resources and procedures such as the ability to deal with suspected or actual breaches and take remedial action. There should also be process modifications to mitigate risk and prevent future breaches.

20. In particular, Jurisdictions' domestic legal framework should enable the imposition of adequate and appropriate penalties and/or sanctions for improper disclosure or use of taxpayer information, including exchanged information, with an appropriate consideration of administrative, civil, and criminal penalties or sanctions.

21. Furthermore, Jurisdictions should:

- have processes to follow when there is suspected or actual unauthorised access, use or disclosure, which should ensure such issues are reported and investigated;
- with the support of adequate administrative resources, processes and procedures, ensure that remedial action is taken where actual issues have been identified, with appropriate penalties or sanctions applied in practice against employees, contractors and other persons who violate confidentiality rules, security policies or procedures, to deter others from engaging in similar violations;
- apply processes to notify other Competent Authorities of breaches of confidentiality or failure of safeguards, and of sanctions and remedial actions consequently imposed; and
- review the monitoring and enforcement processes in response to non-compliance, with senior management ensuring that recommendations for change are implemented in practice.

Commentary on Section 6 concerning Consultations and Amendments

Paragraph 1 – Consultations

1. This paragraph provides that if any difficulties in the implementation or interpretation of the CARF MCAA arise, either Competent Authority may request consultations to develop measures to ensure that

the CARF MCAA is fulfilled. Consultations may also be held to analyse the quality of the information received.

2. The Competent Authorities may communicate with each other for purposes of reaching an agreement on appropriate measures to ensure that the CARF MCAA is fulfilled. The Co-ordinating Body Secretariat will notify all Competent Authorities, including those that did not participate in the consultation, of any measures developed to ensure the CARF MCAA is fulfilled.

Paragraph 2 – Amendments

3. This paragraph clarifies that the CARF MCAA may be amended by written agreement of the Competent Authorities. Unless the Competent Authorities otherwise agree, such amendment is effective on the first day of the month following a period of one month after the date of the last signature of such written agreement.

Commentary on Section 7 concerning General Terms

Paragraph 1 – Notifications

1. Paragraph 1 describes the notifications that, at the time of signing the CARF MCAA or as soon as possible thereafter, a Competent Authority must provide to the Co-ordinating Body Secretariat before the CARF MCAA can take effect with respect to another Competent Authority:

- the notification under subparagraph 1a) is a confirmation that the Jurisdiction has the necessary laws in place to implement the Crypto-Asset Reporting Framework, as well as a specification of the relevant effective dates of such legislation. This could include the specification of any conditions in national legislative procedures that may necessitate the provisional application of the CARF MCAA during a limited period. When specifying such provisional application, the notification should set out the state of advancement of the national legislative procedures, the reasons for the provisional application, and the time period, which should in no case extend beyond the end of the first reportable period. This notification should provide assurances that the legislation of the Jurisdiction can ensure the due diligence and reporting requirements of the Crypto-Asset Reporting Framework will be fulfilled with respect to all Reporting Crypto-Asset Service Providers that are subject to such requirements in the Jurisdiction pursuant to Section I of the Crypto-Asset Reporting Framework, notably by including specific references to the underlying legislation that ensures such requirements can be fulfilled;
- the notification under subparagraph 1b) is confirming whether the Jurisdiction should be listed as a reciprocal Jurisdiction, or as a non-reciprocal Jurisdiction (e.g. because the jurisdiction does not have a direct tax system or because the Competent Authority of the Jurisdiction does not meet an appropriate level of confidentiality and data safeguards). While a non-reciprocal Jurisdiction would be required to send information foreseen under Section 2, it would not receive information from other Competent Authorities. A Competent Authority should file its notification of intention for non-reciprocity even if this is only temporary (e.g. pending an assessment of its confidentiality and data safeguards);
- the notification under subparagraph 1c) provides for a declaration by the Competent Authority requesting consent from the other Competent Authorities to use the information received under the CARF MCAA for the assessment, collection or recovery of, the enforcement or prosecution in respect of, or the determination of appeals in relation to taxes with respect to which its Jurisdiction made a reservation pursuant to subparagraph 1(a) of Article 30 of the Convention. The requesting Competent Authority should specify these taxes and confirm the use will be in line with the terms of the Convention. The other Competent Authority must explicitly agree with

such use as part of listing the requesting Competent Authority as an intended exchange partner in the notification provided pursuant to subparagraph 1g);

- in the fourth notification provided under subparagraph 1d), the Competent Authorities should indicate whether it wishes to rely on any transmission and encryption methods other than the OECD Common Transmission System and the related file preparation and encryption methods;
- the notification under subparagraph 1e) states that the Jurisdiction should specify any requirements for the protection of personal data that must be respected in the receiving Jurisdiction with respect to information it sends to Competent Authorities in such Jurisdictions, in addition to the confidentiality and use limitation requirements contained in Article 22 of the Convention. This allows the sending Competent Authority to condition the sending of any information on the confirmation of specified safeguards being in place in the receiving Jurisdiction. The other Competent Authority must explicitly agree with such safeguards as part of listing the sending Competent Authority as an intended exchange partner in the notification provided pursuant to subparagraph 1g). Alternatively, under this notification, a Competent Authority can also simply indicate that it does not wish to make any further specifications with respect to data protection safeguards;
- the notification under subparagraph 1f) requires that Jurisdictions confirm whether it has in place adequate measures to ensure the required confidentiality and data safeguards standards, as discussed in Section 5, are met. This can be confirmed by referring to the relevant Confidentiality and Data Safeguards Report for the Jurisdiction, as adopted by the Global Forum on Transparency and Exchange of Information for Tax Purposes;
- finally, in the notification under subparagraph 1g), the Competent Authority should include a list of the Jurisdictions of the Competent Authorities with respect to which it intends to have the CARF MCAA in effect, following national legislative procedures for entry into force (if any). When including a Jurisdiction on this list, it also agrees to comply with the data protection requirements as notified by the Competent Authority of such Jurisdiction pursuant to subparagraph 1e). In addition, where relevant, the Competent Authority can specify in this notification whether it agrees with the use of information it is exchanging with the Competent Authority of another Jurisdiction for the administration of enforcement of taxes set out in the notification under subparagraph 1c).

2. In addition to providing these notifications set out above, paragraph 1 clarifies that Competent Authorities must notify the Co-ordinating Body Secretariat, promptly, of any subsequent changes to be made to the above-mentioned notifications, once they have been lodged.

Paragraph 2 – Entry into effect

3. Paragraph 2 provides that a specific bilateral exchange relationship is activated and enters into effect on the date the second of the two Competent Authorities provides all notifications required under paragraph 1 to the Co-ordinating Body Secretariat and has listed the other Competent Authority's Jurisdiction pursuant to subparagraph 1g) of Section 7.

Paragraphs 3 and 4 – Role of Co-ordinating Body Secretariat

4. Paragraph 3 clarifies that the Co-ordinating Body Secretariat will maintain a list of the Competent Authorities that have signed the CARF MCAA, as well as between which Competent Authorities the CARF MCAA is in effect. This information is published on the OECD website.

5. Paragraph 4 further explains that the Co-ordinating Body Secretariat will also publish on the OECD website the notifications filed under subparagraph 1a) (confirming that the Jurisdiction has the necessary laws in place), subparagraph 1b) (confirming whether the Jurisdiction is to be listed as a non-reciprocal

Jurisdiction) and subparagraph 1e) (specifying data protection requirements) of Section 7. The Co-ordinating Body Secretariat will also maintain the information provided by Competent Authorities pursuant to subparagraphs 1c), 1d), 1f) and 1g) of Section 7. This information, however, will not be published on the OECD website and will only be made available to the signatories of the CARF MCAA.

Paragraph 5 – Suspension

6. Paragraph 5 provides details on the possibility for a Competent Authority to suspend the CARF MCAA in relation to another Competent Authority when it has determined that there is or has been significant non-compliance by that other Competent Authority. Where possible, the Competent Authorities should try to resolve any issues of non-compliance, even those of significant non-compliance, before issuing a notification to suspend the CARF MCAA between them.

7. To suspend the CARF MCAA, a Competent Authority must notify the other Competent Authority in writing that it intends to suspend the CARF MCAA with such other Competent Authority. The notification should, whenever possible, set out the reasons for the suspension and the steps (to be) taken to resolve the issue. The suspension will have immediate effect.

8. The notified Competent Authority should, as soon as possible, undertake the necessary steps to address the significant non-compliance. As soon as the non-compliance is resolved, the notified Competent Authority should advise the other Competent Authority. Following successful resolution of the issue, the Competent Authority that sent the suspension notification should confirm in writing to the notified Competent Authority that the CARF MCAA is no longer suspended and exchanges of information should recommence as soon as possible.

9. Paragraph 5 provides that significant non-compliance includes, but is not limited to:

- non-compliance with the confidentiality or data safeguard provisions of the CARF MCAA, for example information is used for purposes not authorised in the CARF MCAA or the Convention or domestic legislation is amended in such a way that the confidentiality of information is compromised; or
- a failure by the Competent Authority to provide timely or adequate information as required under the CARF MCAA.

10. During the period of any suspension all information previously received under the CARF MCAA will remain confidential and subject to the terms of Section 5 of the CARF MCAA, including any additional data safeguards specified by the supplying Competent Authority.

Paragraph 6 – Deactivation and termination

11. Pursuant to paragraph 6, a Competent Authority may either deactivate a particular exchange relationship under the CARF MCAA or entirely terminate its participation in the CARF MCAA. In both instances the Competent Authority must notify the Co-ordinating Body Secretariat in writing. A deactivation or termination will become effective on the first day of the month following the expiration of a period of 12 months after the date of the notification. In circumstances where this is necessary (e.g. due to national legislative procedures or a court judgement), the Competent Authority deactivating one or more exchange relationships under, or terminating its participation in, the CARF MCAA, may deviate from the default 12 month period and specify another period.

12. The termination of the participation of a Jurisdiction in the Convention would lead to the automatic termination of the CARF MCAA in respect of such Jurisdiction. Accordingly in such circumstances the CARF MCAA would not separately need to be terminated.

13. Paragraph 6 clarifies that in the event of a deactivation or termination, all information previously received under the CARF MCAA will remain confidential and subject to the terms of Section 5, including any additional data safeguards specified by the supplying Competent Authority.

Commentary on Section 8 concerning the Co-ordinating Body Secretariat

1. Section 8 clarifies that, unless otherwise provided for in the CARF MCAA, the Co-ordinating Body Secretariat will notify all Competent Authorities of any notifications that it has received under the CARF MCAA. Section 8 also clarifies that the Co-ordinating Body will notify all signatories of the CARF MCAA when a new Competent Authority signs the CARF MCAA.

Note

[1] See EU General Data Protection Regulation (GDPR) 2016/679 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434