A. Commentaries on the Model Competent Authority Agreement

Introduction

1. The Model CAA links the CRS and the legal basis for the exchange (such as the Convention on Mutual Administrative Assistance in Tax Matters or a bilateral tax treaty). The Model CAA consists of a preamble and seven sections and provides for the modalities of the exchange to ensure the appropriate flows of the information. The preamble contains representations on domestic reporting and due diligence rules that underpin the exchange of information pursuant to the Model CAA. It also contains representations on confidentiality, safeguards and the existence of the necessary infrastructure for an effective exchange relationship.

2. The Model CAA contains a section dealing with definitions (Section 1), covers the type of information to be exchanged (Section 2), the time and manner of the exchange (Section 3) ,collaboration on compliance and enforcement (Section 4) and the confidentiality and data safeguards that must be respected (Section 5). Consultations between the Competent Authorities, amendments to the Agreement and term of the Agreement, including suspension and termination, are dealt with in Sections 4, 6 and 7.

3. The Model CAA is drafted as a bilateral reciprocal agreement based on the principle that automatic exchange is reciprocal and that the exchange will be done on a bilateral basis. To reduce the costs associated with signing multiple competent authority agreements the exchange of information could also be implemented on the basis of a multilateral competent authority agreement/arrangement. A multilateral version of the Model CAA is included as Annex 1. Although the agreement would be multilateral the exchange of information itself would be on a bilateral basis. Further there may be instances where jurisdictions wish to enter into a non-reciprocal bilateral agreement (e.g. where one jurisdiction does not have an income tax). A nonreciprocal version of the Model CAA is included as Annex 2. It has been

acknowledged, by the G20 and others, that developing countries may face particular capacity issues as regards automatic exchange of information and that this is an important issue which needs to be addressed and in July 2013 the G20 called on the Global Forum on Transparency and Exchange of Information for Tax Purposes to work with the OECD Task Force on Tax and Development, the World Bank and others to help developing countries identify their need for technical assistance and capacity building.

4. Jurisdictions could also enter into a multilateral intergovernmental agreement or multiple intergovernmental agreements that would be international treaties in their own right or regional legislation covering both the reporting obligations and due diligence procedures coupled with a more limited competent authority agreement.

Commentary on the Preamble

1. The preamble ("whereas clauses") provide relevant context and representations including a sentence referring to the underlying legal basis that permits the automatic exchange of information.

2. The first clause serves as an introduction and may vary depending on the particular circumstances of the jurisdictions entering into the Agreement.

3. The second clause sets out the representations by the Competent Authorities that the laws of their respective jurisdictions require, or are expected to require, financial institutions to report information regarding certain accounts, consistent with the scope of exchange contemplated by Section 2 of this Agreement.

4. The alternative language used in this clause allows jurisdictions, that so wish, to sign the competent authority agreement even before one or both of the jurisdictions have the relevant rules on due diligence and reporting in place. See also paragraph 3 of Section 3 (paragraph 3 of the Commentary on Section 3) and Section 7 (paragraph 1 of the Commentary on Section 7).

5. The third clause sets out the legal basis that authorises the automatic exchange of financial account information and allows the Competent Authorities to agree the scope and modalities of such automatic exchanges. The scope agreed to must be consistent with the scope of exchange contemplated by Section 2 of this Agreement. Other legal instruments (i.e. instruments other than income tax conventions or the Convention on Mutual Administrative Assistance in Tax Matters) that permit the automatic exchange of information for tax purposes include certain tax information exchange agreements, or regional tax co-operation agreements. On a regional basis the automatic exchange of information could also be implemented on the basis of e.g. EU law or Andean community legislation that covered the elements of the Model CAA and the CRS.

6. The fourth clause sets out the representations by the Competent Authorities that they 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. The Commentary on Section 5 of the Model CAA provides more information.

Commentary on Section 1 concerning Definitions

Paragraph 1 – Definitions

1. Paragraph 1 contains the definitions of the terms that are specific to the Agreement. The definitions of all the other terms used in the Agreement are contained in Section VIII of the Common Reporting Standard.

2. Subparagraphs 1(a) and (b) are intended to include the description of the jurisdictions concluding the Agreement. Competent Authorities are free to agree on the definitions of the terms "[Jurisdiction A]" and "[Jurisdiction B]"; however, such definitions must be consistent with the definitions contained in the underlying legal instrument. Furthermore, Competent Authorities are free to include a geographic description (including a reference to continental shelves); however, only a political definition is necessary. An example of a political definition is "Mexico means the United Mexican States".

3. The definition of the term "Competent Authority" contained in subparagraph 1(c) is intended to include a description of the competent authorities for purposes of the Agreement. This definition enables each jurisdiction to designate one or more authorities as being competent. However, such definition must be consistent with the definition contained in the underlying legal instrument.

4. The terms contained in subparagraphs 1(d) through (k) align the scope of the exchange of information between the jurisdictions concluding the Agreement to the scope of the Common Reporting Standard. Such terms refer to:

- the financial institutions required to report: "[Jurisdiction A] Financial Institution", "[Jurisdiction B] Financial Institution", and "Reporting Financial Institution", which are consistent with the terms "Reporting Financial Institution" and "Participating Jurisdiction Financial Institution" contained in subparagraphs A(1) and (2) of Section VIII of the Common Reporting Standard (see paragraphs 2-6 of the Commentary on Section VIII);

- the financial accounts reported: "Reportable Account", "[Jurisdiction A] Reportable Account", and "[Jurisdiction B] Reportable Account", which are consistent with the term "Reportable Account" contained in subparagraph D(1) of Section VIII of the Common Reporting Standard (see paragraph 105 of the Commentary on Section VIII); and
- the account holders subject to reporting: "[Jurisdiction A] Person" and "[Jurisdiction B] Person", which are consistent with the terms "Reportable Person" and "Reportable Jurisdiction Person" contained in subparagraphs D(2) and (3) of Section VIII of the Common Reporting Standard (see paragraphs 106-116 of the Commentary on Section VIII).

5. Subparagraph 1(l) contains the definition of the term "TIN", which is also a term defined in subparagraph E(5) of Section VIII of the Common Reporting Standard. Whilst the latter is intended to describe that a TIN is a Taxpayer Identification Number or a functional equivalent in the absence of a Taxpayer Identification Number (see paragraphs 146-149 of the Commentary on Section VIII), the purpose of the former is to identify the TINs of the jurisdictions concluding the Agreement. The terms "[Jurisdiction A] TIN" and "[Jurisdiction B] TIN" contained in subparagraphs 1(m) and (n) also serve this purpose.

6. The term "Common Reporting Standard" is not defined in the Model Competent Authority Agreement, but it is defined in the multilateral version of the Model Competent Authority Agreement. It is possible that the Common Reporting Standard, including the IT modalities, will be updated from time to time as more jurisdictions implement, and obtain experience with, the Common Reporting Standard. In the context of a multilateral agreement competent authorities may sign on different dates and because of the differing dates of signature the Common Reporting Standard may have been updated in the interim. To address this situation, the multilateral version defines the Common Reporting Standard as "the standard for automatic exchange of financial account information developed by the OECD, with G20 countries, presented to the G20 in 2014 and published on the OECD website". In addition, to ensure that there is an understanding that all jurisdictions would be expected to implement the most recent version of the Standard, the third recital states that it is "expected that the laws of the Jurisdictions would be amended from time to time to reflect updates to the Common Reporting Standard and once such changes are enacted by a Jurisdiction the definition of "Common Reporting Standard" would be deemed to refer to the updated version in respect of that Jurisdiction". In a bilateral agreement, the same issue does not arise as competent authorities would generally sign on the same date. However, even in a bilateral agreement, competent authorities may wish to explicitly provide for updates to the Common Reporting Standard

in the same way as set out in the multilateral version (i.e. define the term "Common Reporting Standard" and add a recital setting out the expectation that jurisdictions would amend their laws to reflect updates to the Common Reporting Standard).

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 Model CAA but not defined therein are meant to be interpreted consistently with the meaning given to them in the Common Reporting Standard. This reflects the notion, also expressed in the preamble, that the jurisdictions have introduced reporting and due diligence procedures (including related definitions) consistent with the Common Reporting Standard.

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 this Agreement or in the Common Reporting Standard has the meaning that it has at that time under the law of the jurisdiction applying the Agreement. 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 Common Reporting Standard and any terms defined therein.

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

1. This Section provides that the information to be exchanged is the information required to be reported under the reporting and due diligence rules of the Common Reporting Standard. See Section I (General Reporting Requirements) of the CRS and the related Commentary.

2. The first paragraph refers to the legal basis for the exchange and provides 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 Financial Institution, 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 the CRS and is further specified in paragraph 2.

3. Paragraph 1 makes clear that the exchange of information is subject to the applicable reporting and due diligence rules of the CRS. Thus, where those rules do not require the reporting of, for instance, a TIN with respect to a particular Reportable Account, there is also no obligation to exchange such information. See the exceptions contained in paragraphs C through F of Section I of the CRS and paragraphs 25-35 of the Commentary on Section I.

4. Subparagraph 2(d) of Section 2 provides that a jurisdiction is required to exchange the account balance or value as of the end of the calendar year or other appropriate reporting period. However, paragraph 11 of the Commentary on Section I of the CRS provides that jurisdictions may, as an alternative, require financial institutions to report the average account balance or value during the relevant calendar year or other reporting period. Where a jurisdiction requires reporting of the average account balance or value rather than year-end balance, this should be set out in the Agreement, including the applicable rules to determine the average account balance or value, so that it is clear what is being exchanged.

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

Paragraphs 1 and 2 – Amount, characterisation and currency of payments

1. Paragraph 1 provides that for the purposes of the exchange of information in Section 2, the amount and characterisation of payments made with respect to a Reportable Account may be determined in accordance with the principles of the tax laws of the jurisdiction sending the information. Paragraph 2 provides that the information exchanged will identify the currency in which each amount is denominated.

Paragraphs 3 and 4 – Time of exchange of information

2. Paragraph 3 provides that the information 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 left blank and is for jurisdictions to insert. The nine-month timeline in paragraph 3 is a minimum standard and jurisdictions are free to agree on shorter timelines. For example, Member States of the European Union are subject to a 6-month timeline under the Savings Directive.

3. Paragraph 3 also provides that notwithstanding the year that the Competent Authorities have chosen 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 effect legislation that requires reporting with respect to such calendar year that is consistent with the scope of exchange provided for in Section 2 and in the Common Reporting Standard. This sentence will not be operational if at the time the Agreement is signed both jurisdictions have in effect domestic legislation consistent with the Common Reporting Standard. If one or both of the jurisdictions do not have such legislation in place at the time of signature, the sentence will operate to ensure that once the Agreement has come into effect but the Common Reporting Standard has been in place for longer in

one of the jurisdictions, the only information that needs to be exchanged is years with respect to which both jurisdictions have the relevant reporting obligations in place. A Jurisdiction may however choose, subject to its domestic laws, to exchange with respect to the earlier years in which case this is also consistent with the CRS and the Model CAA.

4. The following example illustrates the operation of paragraph 3 where one jurisdiction does not have legislation requiring reporting in effect for the calendar year that was agreed to in the first sentence of paragraph 3. Jurisdictions A and B sign the Model CAA on 30 April 2015 and agree that information will be exchanged with respect to 2016 and subsequent years. Jurisdiction A provides notice on 7 June 2015 that it has legislation in effect that requires reporting with respect to 2016. Jurisdiction B provides notice on 1 November 2015 that it has legislation in effect to provide reporting with respect to 2017. In this case the last sentence of paragraph 3 will operate such that Jurisdiction A does not have an obligation to exchange information in respect of 2016. Both jurisdictions A and B will have an obligation to exchange information with respect to 2017. However, Jurisdiction A may choose, subject to its domestic laws, to send information to Jurisdiction B in respect of 2016 even though Jurisdiction A will not receive information in respect of 2016.

5. Paragraph 4 contains an exception with respect to the year gross proceeds are to be reported. It may be more difficult for Reporting Financial Institutions to implement procedures to obtain the total gross proceeds from the sale or redemption of property. Thus, when implementing the Common Reporting Standard, jurisdictions may choose to gradually introduce the reporting of such gross proceeds. If no transition is provided, paragraph 4 will be unnecessary. If a transition is provided for by one of the jurisdictions, paragraph 4 should be included which provides that notwithstanding paragraph 3, the information to be exchanged with respect to the year identified in paragraph 3 is the information described in paragraph 2 of Section 2, except for gross proceeds described in subparagraph 2(e)(2) of Section 2. In such a case, jurisdictions should specify the year for which gross proceeds are to be reported.

6. Nothing in the Agreement prevents the application of the provisions of Sections 2 and 3 with respect to the information obtained prior to the effective date of the Agreement, as long as such information is provided after the Agreement is in effect and the provisions of Sections 2 and 3 have become effective. Competent Authorities may find it useful, however, to clarify the extent to which the provisions of Sections 2 and 3 are applicable to such information.

Paragraphs 5 and 6 – Information Technology modalities

CRS schema and user guide

7. Paragraph 5 provides that the Competent Authorities will automatically exchange the information described in Section 2 in a common reporting standard schema in Extensible Markup Language. Guidance on the relevant schema and its use is contained in the CRS user guide, which is included in Annex 3.

Data transmission including encryption

8. Paragraph 6 provides that the Competent Authorities will agree on one or more methods for data transmission, including encryption standards.

Appropriate minimum standards

9. Any transmission method should meet appropriate minimum standards to ensure the confidentiality and integrity of data throughout the transmission. Confidentiality means that data or information is not made available or disclosed to unauthorised persons. Integrity means that data or information has not been modified or altered in an unauthorised manner. Such standards should be susceptible to changing technological capabilities over time. This includes the use of secure transmission channels and protocols that ensure confidentiality and integrity of the data through encryption or physical measures or a combination of both.

10. The Model CAA does not mandate a single solution for data transmission or encryption, as this could limit the ability of Competent Authorities to agree systems and practices that are already successfully in use or may be appropriate in the particular circumstances. As the responsibility for the data remains with the sending jurisdiction until the data reaches the receiving jurisdiction, it is also possible that, depending on national requirements, different processes may be agreed for the two parts of a bilateral exchange (i.e. sending and receiving). For example, jurisdiction A may use browser based transmission and jurisdiction B a server routed through a secure network to exchange data. However, given that jurisdictions would enter into CRS based automatic exchange relationships with a number of jurisdictions, thought will need to be given to designing a sustainable international transmission architecture that mitigates the need for each jurisdiction having to potentially adopt and maintain multiple methods of transmission and/or encryption.

Encryption

11. Encryption is designed to protect both the confidentiality and the integrity of data. It ensures that data is transformed in order to render it unintelligible to anyone who does not possess the decryption key. All data files to be exchanged should therefore be encrypted to a minimum secure standard, and the transmission path should be encrypted or otherwise physically secured with audit controls in place to monitor access and file copies. 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.

Electronic transmission methods

12. While it used to be common to send encrypted files of data on floppy discs, memory sticks and compact discs by physical handover or signed-for postal mail between Competent Authorities, additional administration and risk attach to transfer of portable media (even when integrity and confidentiality are assured by encryption). It is now technologically as straightforward to transfer data using an internet browser which can also inexpensively provide encryption, non-revocation and non-repudiation capabilities, so use of portable media would no longer be considered best practice. A transmission method that allows an integrated end-to-end transfer process for transmission of electronic files is the recommended best practice, whether server-to-server or browser based.[1] Secure email under minimum standards and specifications may alternatively be used, but may have higher installation costs or operating complexity in managing user accesses and data security, including file size

1. WEB SERVICES with ws-security is another affordable standard coming to be widely used in secure environments, formed by a set of services using HTTP protocol through standard methods such as GET and POST. Examples of transmission protocols that have been agreed internationally to meet requirement for secure transmission channels and protocols that ensure confidentiality and integrity of the data include transport layer security (TLS) v 1.1 for secure browser based exchanges and secure file transfer protocol (SFTP) for scheduled bulk transfer, but these are not the only protocols that may provide appropriate solutions.

limits and firewall issues. The importance of risk assessment and continuous reassessment of risk should be recognised.

Operational security implementation

13. The confidentiality and security of data transmitted also depends on good managerial, organisational and operational procedures, as well as technical measures such as hardware and software tools. Although conformance with any particular standard is not mandated, ideally security should be managed in a manner that is consistent with best practice standards such as the ISO 27000 series Information Security standards as modified from time to time. More specifically, the data must be accessed only by authorised parties in the transmission process and access to any encryption keys, particularly the private key must be tightly controlled. Evidence of all authorised access to the data or keys should be maintained as an audit log. Further information on data safeguarding and confidentiality standards is contained in the Commentary on Section 5.

Commentary on Section 4 concerning Collaboration on Compliance and Enforcement

1. This Section deals with 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 Financial Institution that Competent Authority should notify the other Competent Authority. The notified Competent Authority will take all appropriate measures available under its domestic law to address the errors or non-compliance described in the notice. See the Commentary on Section IX of the Common Reporting Standard regarding the rules and administrative procedures that jurisdictions must have in place to ensure that the CRS is effectively implemented.

2. The notice under this Section must be in writing and 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 notice from the other Competent Authority. If the issue has not been resolved, the Competent Authority should provide the other Competent Authority with updates every 90 days. If however, after reviewing and considering the notice in good faith, the notified Competent Authority does not agree that there is, or has been, an error or non-compliance as described in the notice it should, as soon as possible, advise the other Competent Authority in writing of such determination and explain the reasons for it.

3. Section 4 does not contemplate direct contact between the Competent Authority from one jurisdiction with a Reporting Financial Institution in the other jurisdiction. As an alternative, two competent authorities may wish to allow for direct contact between a competent authority in one jurisdiction and a Reporting Financial Institution in the other jurisdiction in case of administrative or other minor errors. The decision to include such option will depend on the domestic law in the respective jurisdictions and may also be influenced by the volume of inquiries that a Competent Authority expects

to receive. If the Competent Authorities agree to such an approach, the following language would replace the current language of Section 4:

1. A Competent Authority may make an inquiry directly to a Reporting Financial Institution in the other jurisdiction where it has reason to believe that administrative errors or other minor errors may have led to incorrect or incomplete information reporting. A Competent Authority will notify the other Competent Authority when the first-mentioned Competent Authority makes such an inquiry of a Reporting Financial Institution in the other jurisdiction.

2. A Competent Authority will notify the other Competent Authority when the first-mentioned Competent Authority has reason to believe that there is non-compliance by a Reporting Financial Institution with the applicable reporting requirements and due diligence procedures consistent with the Common Reporting Standard. The notified Competent Authority will take all appropriate measures available under domestic law to address the non-compliance described in the notice.

4. It is the domestic law of the jurisdiction of the Reporting Financial Institution, including protection of personal data that would be applicable to such direct contact.

Commentary on Section 5 concerning Confidentiality and Data Safeguards

1. Confidentiality of taxpayer information has always been a fundamental cornerstone of tax systems. Both taxpayers and tax administrations have a legal right to expect that information exchanged remains confidential. In order to have confidence in their tax systems and comply with their obligations under the law, taxpayers need to know that the often sensitive financial information is not disclosed inappropriately, whether intentionally or by accident. Citizens 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 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.[2] Several jurisdictions have specific rules on the protection of personal data which also apply to taxpayer information.

2. Section 5 together with Section 7 and the representations in the fourth clause of the preamble explicitly recognise the importance of confidentiality and data safeguards in connection with the automatic exchange of financial account information. The remainder of this Commentary briefly discusses paragraphs 1 and 2 followed by a comprehensive discussion of confidentiality and data safeguarding in connection with the Common Reporting Standard.

2. OECD (2012), *Keeping it Safe: The OECD Guide on the Protection of Confidentiality of Information Exchanged for Tax Purposes*, OECD, Paris, available on www.oecd.org/ctp/exchange-of-tax-information/keeping-it-safe-report.pdf.

Paragraph 1 – Confidentiality including protection of personal data

3. All information exchanged is subject to the confidentiality rules and other safeguards provided for in the underlying legal instrument. This includes the purposes for which the information may be used and limits to whom the information may be disclosed.

4. Many jurisdictions have specific rules on the protection of personal data 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). 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. Paragraph 1 of Section 5 provides that the supplying Competent Authority may, to the extent needed to ensure the necessary level of protection of personal data, specify in the Competent Authority Agreement the particular safeguards that must be respected, as required under its domestic law. The Competent Authority receiving the information must ensure the practical implementation and observance of any safeguarding specified. 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. 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.

5. Exchange of information instruments 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.[3] While it is rare for this to apply in the context of information exchange between Competent Authorities, certain jurisdictions may require their Competent Authorities to specify that information it supplies 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) as that would contravene the public

3. See for example subparagraph 3(c) of Article 26 of the OECD Model Tax Convention and subparagraph 2(d) of Article 21 of the Multilateral Convention on Mutual Administrative Assistance in Tax Matters.

policy of the supplying jurisdiction. In such a case, a provision to this effect could be included in the Competent Authority Agreement.

Paragraph 2 – Breach of confidentiality

6. Ensuring the 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 (including the additional safeguards (if any) specified by the supplying Competent Authority) the Competent Authority must immediately notify the other Competent Authority 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 (if any) specified by the supplying Competent Authority) would be considered significant non-compliance and a justification for immediate suspension of the Competent Authority Agreement.

Confidentiality and data safeguards under the Common Reporting Standard

7. Three building blocks are essential in ensuring appropriate safeguards are in place to protect the information exchanged automatically: *(i)* the legal framework, *(ii)* information security management: practices and procedures, and *(iii)* monitoring compliance and sanctions to address a breach of confidentiality. Each one of these aspects is discussed further below. Annex 4 is a questionnaire[4] which translates the discussion into a series of questions and which jurisdictions may find a useful tool in assessing whether the required confidentiality and data safeguards are met. Jurisdictions may choose to design their own questionnaire to translate the principles of the confidentiality and data safeguard aspects of the CRS. Other jurisdictions may choose not to use a questionnaire as they already have an ongoing automatic exchange of information relationship with another jurisdiction and have previously satisfied themselves that the partner jurisdiction has appropriate safeguards in place to protect the information exchanged automatically.

4. The example questionnaire in Annex 4 is the questionnaire used by the United States for the purposes of FATCA as of 20 March 2014 with the United States specificities removed.

1. Legal Framework

8. The legal framework must ensure the confidentiality of exchanged tax information and limit its use to appropriate purposes in accordance with the terms of the exchange instrument. The two basic components of such a framework are the terms of the applicable instrument and a jurisdiction's domestic legislation.

9. All bilateral and multilateral tax conventions and other legal instruments under which tax information is exchanged must contain provisions requiring that the confidentiality of exchanged information be maintained and that its use be limited to certain purposes. The OECD Model Tax Convention is illustrative. Paragraph 2 of Article 26 of the Model Tax Convention requires that taxpayer information received by a Competent Authority be treated as secret in the same manner as taxpayer information obtained under the jurisdiction's domestic laws. The disclosure of such information is restricted to "persons or authorities (including courts and administrative bodies)" involved in assessment, collection, administration, or enforcement of covered taxes, or in related prosecutions, appeals or oversight. It also allows use for another purpose if authorised by both competent authorities and if the laws of both states permit such use. Similarly Article 22 of the Multilateral Convention on Mutual Administrative Assistance in Tax Matters requires that information be treated as secret and protected in the same manner as information obtained under the domestic law of the party and imposes limitations on the use and disclosure of the information.

10. Domestic legislation must include provisions sufficient to protect the confidentiality of taxpayer information and provide for specific and limited circumstances under which such information can be disclosed and used. Domestic law must also impose significant penalties or sanctions for improper disclosure or use of taxpayer information. Further, domestic law must provide that the jurisdiction's international exchange instruments are legally binding, such that confidentiality obligations in such instruments are also binding. Additionally, a jurisdiction's domestic law for safeguarding taxpayer data must apply to taxpayer information received from another government under an exchange instrument.

2. Information Security Management: Practices and Procedures

11. In order for the legal protections afforded under the exchange instrument and domestic law to be meaningful, practices and procedures must be in place to ensure that exchanged taxpayer information can be used solely for tax purposes (or other specified purposes) and to prevent the disclosure of taxpayer information to persons or governmental authorities that

are not engaged in the assessment, collection, administration, or enforcement of covered taxes, or in related prosecutions, appeals or oversight.

12. An information security management system is a set of policies, practices and procedures concerned with information security management including IT related risks. This is not just a technical issue but also a management, cultural and organisational issue. As discussed in more detail below the practices and procedures implemented by tax administrations should cover all aspects relevant to protecting confidentiality including a screening process for employees handling the information, limits on who can access the information and systems to detect and trace unauthorised disclosures. The information security management practices and procedures used by each jurisdiction's tax administration must adhere to internationally recognised standards or best practices that ensure the protection of confidential taxpayer data.[5] More specifically this would include the following baseline controls:

2.1. Employees (background checks, employment contracts, training)

13. Tax administrations must ensure that individuals in positions of authority and access are trustworthy and meet security criteria, and their access privileges are appropriately managed and monitored. Employees, consultants and others with access to confidential information must be screened for potential security risks. Consultants with access to taxpayer information must be contractually bound by the same obligations as employees to keep taxpayer information confidential.

14. Tax administrations must also ensure that employees with access to data are aware of the confidentiality requirements of their positions, the security risks associated with their activities, and applicable laws, policies, and procedures related to security/confidentiality. As long as employees continue to have access to data, annual or more frequent training must continue.

5. The internationally accepted standards for information security are known as the "ISO/IEC 27000-series", which are published jointly by the International Organisation for Standardisation (ISO) and the International Electro-technical Commission (IEC). The series provides best practices on information security management, risks, and controls within the context of an overall information security management system. A tax administration should be able to document readily that it is compliant with the ISO/IEC 27000-series standards or that it has an equivalent information security framework and that taxpayer information obtained under a legal instrument is protected under that framework.

15. In addition, there must be procedures in place to quickly end access to confidential information for terminated, transferred, or retired employees who no longer need such access. Further, confidentiality obligations must continue after access has ceased.

2.2. Access to premises and physical document storage

16. Tax administrations must have security measures in place to restrict entry to their premises. Measures often include the presence of security guards, policies against unaccompanied visitors, security passes, or coded entry systems for employees and limits on employee access to areas where sensitive information is located.

17. Tax administrations must also provide secure storage for confidential documents. Information can be secured in locked storage units or rooms, such as cabinets (whether locked with combinations or keys), safes and strong rooms. Access to combinations and keys must be limited. The security of physical storage cabinets must vary depending on the classification of their contents, and bulk tax data exchanged automatically must have an appropriate security classification. Tax administrations must also ensure this security continues when data is taken to alternate work sites.

2.3. Planning

18. Tax administrations must have a plan to develop, document, update, and implement security for information systems.

2.4. Configuration Management

19. Tax administrations must control and manage the configuration of information systems. To this end, they must develop, document, disseminate, and update relevant security controls.

2.5. Access Control

20. Tax administrations must limit system access to authorised users and devices (including other information systems). Authorised users must be limited to accessing the transactions and functions they are permitted to undertake.

2.6. Identification and Authentication

21. Information systems must have the means to store and authenticate the identities of users and devices that require access to information systems. Information systems must also be capable of identifying an unauthorised user and preventing him or her from accessing confidential information.

2.7. Audit and Accountability

22. Unauthorised users can be held accountable only if their actions are traceable. Therefore, it is essential for tax administrations to create and retain information system audit records for monitoring, analysing, investigating, and reporting of unlawful, unauthorised, or inappropriate information system activity.

2.8. Maintenance

23. Tax administrations must perform periodic and timely maintenance of systems, and provide effective controls over the tools, techniques, and mechanisms for system maintenance and the personnel that use them.

2.9. System and Communications Protection

24. Tax administrations must monitor, control, and protect communications at external and internal boundaries of information systems. These controls must include procedures to remove residual data, provide transmission confidentiality, and validate cryptography.

2.10. System and Information Integrity

25. Tax administrations must identify, report, and correct (or take remedial action for) information communication technology security incidents in a timely manner, providing protection from malicious code and monitoring system security alerts and advisories.

2.11. Security Assessments

26. The tax administration must develop and regularly update a policy for reviewing the processes used to test, validate, and authorise the security controls for protecting data, correcting deficiencies and reducing vulnerabilities. The frequency of such updates will be risk-based but must be done at appropriate intervals in line with internationally recognised standards or best practices. It must also have a policy to review the manner in which

information system operations and connections are authorised, and the procedures for monitoring system security controls.

2.12. Contingency Planning

27. Tax administrations must establish and implement plans for emergency response, backup operations, and post-disaster recovery of information systems.

2.13. Risk Assessment

28. A tax administration must assess the potential risk of unauthorised access to taxpayer information, and the risk and magnitude of harm from unauthorised use, disclosure, disruption, modification, or destruction of such information or of the taxpayer information systems. It must update its risk assessment periodically or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.

2.14. Systems and Services Acquisition

29. Tax administrations must ensure that third-party providers of information systems that are engaged to process, store, and transmit information exchanged under the legal instrument use security controls consistent with the necessary computer security requirements.

2.15. Media Protection

30. Tax administrations must protect information in printed form or on digital media, limit information access to authorised users, and sanitise or destroy digital media before disposal or reuse.

2.16. Data Identification

31. Data exchanged under the legal instrument must always be protected against inadvertent disclosure. If the data is included in a file that includes other data and physical separation is impractical, procedures must be in place to ensure that the entire file is safeguarded and clearly labelled to indicate the inclusion of data exchanged under a legal instrument. The information itself also must be clearly labelled.

32. Procedures must be in place to ensure that, before such a file is released to an individual or agency not authorised to access data exchanged under a legal instrument, all such data has been removed. In case the data is stored in a database procedures must be in place to ensure that, before access

to the database is provided to an individual or agency not authorised to access data exchanged under a legal instrument, all such data has been deleted from the database (or securely partitioned/protected in a way that prevents the unauthorised individual or agency from accessing that data).

2.17. Information Disposal Policies

33. Tax administrations must have policies requiring data to be destroyed as soon as it is no longer needed and ensuring secure disposal of confidential information. Document shredding, burn boxes, or locked waste bin shredding is appropriate for paper documents, and electronic documents should be deleted when no longer necessary. Confidential information must be removed prior to the disposition of computers and information storage devices.

3. Monitoring compliance and sanctions to address a breach of confidentiality

34. In addition to keeping information exchanged under a legal instrument confidential, tax administrations must be able to ensure that its use will be limited to the purposes defined by the applicable information exchange agreement. Thus, compliance with an acceptable information security framework alone is not sufficient to protect tax data that has been exchanged. In addition, domestic law must impose penalties or sanctions for improper disclosure or use of taxpayer information. To ensure implementation, such laws must be reinforced by adequate administrative resources and procedures.

3.1. Penalties and Sanctions

35. Domestic law must impose penalties or sanctions for improper disclosure or use of taxpayer information, and tax administrations must in fact impose these penalties and sanctions against personnel who violate security policies and procedures to deter others from engaging in similar violations. To ensure implementation, such laws must be reinforced by adequate administrative resources and procedures. Tax administrations should implement a formal sanctions process for personnel and third-party providers who fail to comply with established information security policies and procedures. Policies should consider both civil and criminal sanctions for unauthorised inspection or disclosure.

3.2. Policing Unauthorised Access and Disclosure

36. In addition to having policies that govern access to confidential information, tax administrations must also have processes in place to monitor compliance with these policies and detect any unauthorised access

and disclosure. If it occurs, there must be an investigation followed by the preparation of a report for management. The report must include:

- recommendations for minimising the repercussions of the incident;
- an analysis of how to avoid similar incidents in the future;
- recommendations for any penalties to be imposed on the person(s) responsible for the breach, noting that law enforcement authorities should be involved if intentional disclosure is suspected; and
- reasons for a high degree of confidence that, once implemented, recommended system changes and penalties will prevent similar future breaches.

37. Additionally, tax administrations should have a process for review and approval of recommendations for policy and procedural changes to avoid future breaches. The tax administration's investigating authority or senior management must ensure that approved recommendations are implemented.

Commentary on Section 6 concerning Consultations and Amendments

1. This Section deals with consultations between the Competent Authorities and amendments to the competent authority agreement.

Paragraph 1 – Consultations

2. This paragraph provides that if any difficulties in the implementation or interpretation of this Agreement arise, either Competent Authority may request consultations to develop measures to ensure that this Agreement is fulfilled. Consultations may also be held to analyse the quality of the information received.

3. The Competent Authorities may communicate with each other by letter, facsimile transmission, telephone, direct meetings, or any other convenient means for purposes of reaching an agreement on appropriate measures to ensure that this Agreement is fulfilled.

Paragraph 2 – Amendments

4. This paragraph clarifies that the Agreement 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 next following a period of one month from the later of:

- the date of the signatures of such written agreement, or
- the date that notifications are exchanged for the purposes of such written agreement.

5. As noted in the Introduction to the Commentaries on the Model Competent Authority Agreement jurisdictions could also enter into a multilateral intergovernmental agreement or multiple intergovernmental agreements that would be international treaties in their own right covering both the reporting obligations and due diligence procedures coupled with a more limited competent authority agreement. In such cases different rules regarding amendments may apply.

Commentary on Section 7 concerning Term of Agreement

Paragraph 1 – Entry into force

1. Paragraph 1 provides for two alternatives regarding the effective date. First, where jurisdictions have entered into this agreement after both jurisdictions have the necessary laws in place to implement the Common Reporting Standard, they would decide on a date for the Agreement to come into effect. Second, if the Competent Authorities sign before one or both jurisdictions have the necessary laws in place, they would likely use this second alternative and the agreement would enter into effect on the date of the later of the notifications that the jurisdiction has the necessary rules in place to implement the agreement.

Paragraph 2 – Suspension

2. Paragraph 2 provides details on the possibility for a Competent Authority to suspend the Agreement when it has determined that there is or has been significant non-compliance by the other Competent Authority with this Agreement. Where possible the Competent Authorities should try to resolve any issues of non-compliance, even those of significant non-compliance, before issuing a notice to suspend the operation of the Agreement.

3. To suspend the Agreement a Competent Authority must give notice in writing to the other Competent Authority that it intends to suspend the Agreement. The notice should provide a detailed description of the significant non-compliance that has occurred, or is occurring, and where possible a description of the steps that should be taken to resolve the issue. The suspension will have immediate effect.

4. 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 notice should

confirm in writing to the notified Competent Authority that the Agreement is no longer suspended and exchanges of information should recommence as soon as possible.

5. Paragraph 2 provides that significant non-compliance includes, but is not limited to:

- non-compliance with the confidentiality or data safeguard provisions of this Agreement (including the additional safeguards specified in the Competent Authority Agreement), for example information is used for purposes not authorised in the underlying legal instrument or domestic legislation is amended in such a way that the confidentiality of information is compromised;
- a failure by the Competent Authority to provide timely or adequate information as required under this Agreement;
- defining the status of Excluded Accounts or Non-Reporting Financial Institutions in a manner that frustrates the purposes of the Common Reporting Standard;
- a failure to have rules and administrative procedures in place to ensure the effective implementation of the reporting and due diligence procedures set out in the Common Reporting Standard.

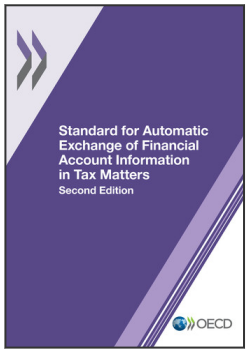
6. During the period of any suspension all information previously received under this Agreement will remain confidential and subject to the terms of Section 5 of the Agreement including any additional data safeguards specified by the supplying Competent Authority and the underlying legal instrument.

Paragraph 3 – Termination

7. Paragraph 3 contains the termination clause. Either Competent Authority may terminate this Agreement by giving notice of termination in writing to the other Competent Authority. Such 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 notice of termination. For example, a Competent Authority may choose to terminate this Agreement when the Agreement has been suspended and the other Competent Authority has not resolved issues of significant non-compliance within a reasonable timeframe.

8. The termination of the underlying legal instrument under which the Competent Authority Agreement is concluded would lead to the automatic termination of the Competent Authority Agreement. Accordingly in such circumstances the Competent Authority Agreement would not separately need to be terminated.

9. Paragraph 3 clarifies that in the event of termination, all information previously received under this Agreement will remain confidential and subject to the terms of Section 5 of the Agreement including any additional data safeguards specified by the supplying Competent Authority and the underlying legal instrument.



From:

Standard for Automatic Exchange of Financial Account Information in Tax Matters, Second Edition

Access the complete publication at:
https://doi.org/10.1787/9789264267992-en

Please cite this chapter as:

OECD (2017), "Commentaries on the Model Competent Authority Agreement", in *Standard for Automatic Exchange of Financial Account Information in Tax Matters, Second Edition*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/9789264267992-6-en

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

You can copy, download or print OECD content for your own use, and you can include excerpts from OECD publications, databases and multimedia products in your own documents, presentations, blogs, websites and teaching materials, provided that suitable acknowledgment of OECD as source and copyright owner is given. All requests for public or commercial use and translation rights should be submitted to rights@oecd.org. Requests for permission to photocopy portions of this material for public or commercial use shall be addressed directly to the Copyright Clearance Center (CCC) at info@copyright.com or the Centre français d'exploitation du droit de copie (CFC) at contact@cfcopies.com.