Ministry of Finance, Trade and the Blue Economy
Liberty House, P.O Box 313/ Victoria/ Mahé, Seychelles

Circular to Seychelles Reporting Financial Institutions

Expert assessment carried out by the Global Forum on Transparency and the Exchange of Information for Tax Purposes on Confidentiality Safeguards implemented within the Seychelles Revenue Commission and DICT in view of the implementation of Automatic Exchange of Information.

I/ Background

At its 7th annual meeting, in October 2014, the Global Forum endorsed the Standard for Automatic Exchange of Financial Account Information in Tax Matters (the AEOI Standard), with a large majority of Global Forum members committing to implement the new standard and to start first exchanges in 2017 or 2018 (including almost all developed countries and financial centres).

Seychelles, which has committed to start the process of exchange in 2017 has therefore to set the framework necessary to the effective implementation of AEOI Standards.

One important aspect of the AEOI Standard and which is key to successful implementation of AEOI is that data and information that is exchanged is kept confidential and appropriately safeguarded from improper use and disclosure.

The implementation of the requirements in this area is necessary if jurisdictions are to have confidence regarding the use of the data they provide and for them to be willing to exchange information.

An important factor in jurisdictions determining with which partners to engage in AEOI will be the measures for confidentiality and data safeguards in these jurisdictions. These issues therefore constitute a key part of the AEOI Standard. The Paragraph 1 of the Commentary to section 5 of the model competent authority agreement contained in the AEOI Standard states as follows:

"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 unauthorized 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.[…]"

All jurisdictions that signed the Multilateral Competent Authority Agreement (MCAA) were therefore required to provide responses to the questionnaire on confidentiality and data safeguards set out at Annex 4 of the AEOI Standard to inform other signatories on the standards in place, in that jurisdiction.

Furthermore, the Global Forum put in place a preliminary assessment process to assess the questionnaire responses from all those implementing the AEOI Standard (whether through the MCAA or bilaterally) to identify any gaps in the standards in place. This includes an assessment by a panel of experts and peer input, focusing on: legislative, operatoinal and information technology standards.

Seychelles, who signed the MCAA and responded to the questionnaire on confidentiality, underwent the assessment in November 2015. The experts came for an on-site visit and met with SRC and DICT officials for interviews and visit of the premises. The purpose of the visit was to assess whether the competent authority has a framework and infrastructure in place to provide comfort that information received through exchanges under the AEOI Standard will, in practice, be kept confidential and will not be used for improper purposes.

II/ Aspects reviewed during the assessment

In accordance with the AEOI Standard, the different elements that were looked at were as follows:

1. ***The legal framework***

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 exchange instrument and the jurisdiction's domestic legislation.

2. ***Information Security Management: Practices and Procedures***

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 other persons or authorities. 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 organizational issue. The information security management practices and procedures used by each jurisdiction's tax administration must adhere to internationally recognized standards or best practices that ensure the protection of confidential taxpayer data. More specifically this would include the following baseline controls:

a) Employees (background checks, employment contracts, training)

b) Access to premises and physical document storage

c) Plans to develop, document, update, and implement security for information systems.

d) Control and management of the configuration of information systems. To this end, SRC must develop, document, disseminate, and update relevant security controls.

e) Access control to limit system access to authorized users and devices (including other information systems). Authorized users must be limited to accessing the transactions and functions they are permitted to undertake.

f) Identification and authentication measures to ensure that 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 unauthorized user and preventing him or her from accessing confidential information.

g) Audit and Accountability procedures for the actions of unauthorized users to be traced.

h) Periodic and timely maintenance of systems, and effective controls over the tools, techniques, and mechanisms for system maintenance and the personnel that use them.

i) System and Communications Protection to ensure the monitoring, control, and protection of communications at external and internal boundaries of information systems. These controls must include procedures to remove residual data, provide transmission confidentiality, and validate cryptography.

j) System and Information Integrity enabling the identification, reporting, and correction of the information communication technology security incidents in a timely manner, providing protection from malicious code and monitoring system security alerts and advisories.

k) Security Assessments

l) Establishment and implementation of plans for emergency response, backup operations, and post-disaster recovery of information systems.

m) Risk Assessment

n) Systems and Services Acquisition to 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.

o) Media Protection

p) Data Identification

q) Information Disposal Policies

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

The experts also had to be satisfied that the information that is exchanged will only be used for the purposes defined by the applicable information exchange agreement. Thus, domestic law must impose penalties or sanctions for improper disclosure or use of taxpayer information, and to ensure implementation, the law must be reinforced by adequate administrative resources and procedures.

Tax administrations must have a process for review and approval of recommendations for policy and procedural changes to avoid future breaches, and the investigating authority or senior management must ensure that approved recommendations are implemented.

III/ Outcome of the assessment

The outcome of the assessment conducted was the endorsement of the data safeguards put in place by Seychelles. This outcome reflects the views of the confidentiality experts in their expert capacity as well as input from all the jurisdictions implementing the AEOI Standard and specifically by the AEOI working group, which has been mandated to ensure a consistent and effective implementation of the AEOI Standard by all the jurisdictions implementing the new Standard.