taxnotes® international

Volume 96, Number 10 ■ December 9, 2019

Why — and How — African Countries Should Use Technology for Automatic Information Exchange

by Jerome Duperrut, Philippe Thevoz, Luukas Ilves, Clement Migai, and Jeffrey Owens

Reprinted from *Tax Notes International*, December 9, 2019, p. 919

Why — and How — African Countries Should Use Technology For Automatic Information Exchange

by Jerome Duperrut, Philippe Thevoz, Luukas Ilves, Clement Migai, and Jeffrey Owens

Jerome Duperrut

Philippe Thevoz

Luukas Ilves

Clement Migai

Jeffrey Owens

Jerome Duperrut is the associate director of economic affairs and international institutions and Philippe Thevoz is vice president of e-government systems with SICPA SA in Lausanne, Switzerland. Luukas Ilves is head of strategy with Guardtime AS in Tallinn. Clement Migai is a research and teaching associate and Jeffrey Owens is the head of the Global Tax Policy Center with the Institute for Austrian and International Tax Law of Vienna University of Economics and Business.

In this article, the authors discuss how digital integrity technologies can help African countries with the automatic exchange of financial account information for tax purposes. They focus on data collection from financial institutions and domestic tax authorities, secure data exchange, blockchain technology, process integrity, and artificial intelligence.

Efforts to enhance global tax transparency have been largely driven by the OECD with the political support of the G-20. The widely adopted international standards on tax transparency are the exchange of information on request (EOIR) and the automatic exchange of financial account information for tax purposes (AEOI). To implement AEOI, each jurisdiction must have domestic and international legal frameworks, meet stringent confidentiality and data safeguard requirements, and operationalize the information exchange network. AEOI is heavily dependent on technological, computing, and administrative capacity, which may be weak in many African countries.

Digital integrity technologies could help fast-track the participation of African countries in the AEOI process and help them leapfrog other countries. They are particularly useful when it comes to the collection and relay of information from financial institutions to tax authorities at the domestic level, the handling of information received by the tax authorities from domestic institutions, meeting the requirements for

confidentiality and data safeguards, and the effective use of information received under AEOI.

Digital integrity technologies optimally address those issues because they cover data, taxpayers, systems, and digital infrastructure. An array of technologies is needed, including blockchain, which acts as the trust anchor. Digital technology should also ensure that data have been generated through the right process. Finally, artificial intelligence can help African countries make sense of the data received under AEOI and use it effectively to generate the proper level of tax revenue.

Introduction

The exchange of information across jurisdictions is essential for tax authorities in their efforts to enhance transparency and combat cross-border tax evasion and avoidance.

The EOIR standard requires that information that is foreseeably relevant for tax purposes be available and accessible to tax authorities, who can then exchange the information with other tax authorities under a legal agreement that can take various forms.[1] It covers information such as identity of legal and beneficial owners of companies, other legal entities, and arrangements like partnerships and trusts; accounting information; and bank account information.

AEOI relies on the common reporting standard (CRS), a single, common global requirement[2] for financial institutions to share financial account information with the tax authorities in the jurisdictions where they are situated, which then exchange that information with their foreign counterparts on an agreed, annual basis. AEOI allows tax authorities to trace financial accounts held in offshore institutions that were previously unknown and unknowable to the home tax authorities.

Developed by the OECD with the political backing of the G-20 in 2014, AEOI commenced in 2017 with 49 jurisdictions exchanging information. An additional 51 jurisdictions started exchanging information in September 2018, bringing the total number of jurisdictions to 100.[3]

The Global Forum on Transparency and Exchange of Information for Tax Purposes monitors and reviews the implementation of both the EOIR (through its peer review process) and AEOI standards.[4] It also supports jurisdictions, mostly developing countries, to enable them to fully participate in AEOI.[5]

Elements Required for Implementing AEOI

To implement the AEOI standard, a participating jurisdiction must have several elements in place.[6]

First, all jurisdictions that want to participate in AEOI must have detailed domestic rules that require financial institutions under its jurisdiction to collect and report the data set out in the CRS and the due diligence procedures they must follow. The institutions collect that information and relay it to their home tax authorities for exchange with foreign authorities with whom they have an agreed, annual exchange relationship.

Second, AEOI requires an international legal framework that enables exchange between agreed partners. Jurisdictions must therefore conclude international agreements with each of their partners to deliver the widespread exchange networks necessary for automatic exchange. Those agreements provide a legal basis for AEOI

[1] The legal mechanisms underpinning the EOIR can be multilateral or bilateral legal instruments. Multilateral legal instruments include the OECD/Council of Europe Multilateral Convention on Mutual Administrative Assistance in Tax Matters or treaties based on the OECD's model tax information exchange agreement. Bilateral mechanisms include tax treaties based on the OECD and U.N. model tax conventions or bilateral versions of the OECD model TIEA.

[2] The OECD developed the CRS in response to a G-20 request, and the OECD Council approved it July 15, 2014. The standard calls on participating jurisdictions to obtain information from their financial institutions and automatically exchange that information with other jurisdictions annually; and sets out financial information to be exchanged, financial institutions subject to reporting requirements, and due diligence procedures to be followed by relevant financial institutions. *See* OECD, "Common Reporting Standard."

[3] Global Forum on Transparency and Exchange of Information for Tax Purposes, "Automatic Exchange of Information: Implementation Report 2018," at 3 (2018); and "Tax Transparency 2018: Report on Progress," at 14 (2018).

[4] For more on the history and work of the global forum, see OECD, "Global Forum on Transparency and Exchange of Information for Tax Purposes."

[5] *See, e.g.*, OECD, "OECD Work on Tax and Development 2018-19," at 23-24 (2019); and "OECD Work on Taxation 2018-19," at 17-19 (2019). *See also* Global Forum, "The Global Forum's Plan of Action for Developing Countries Participation in AEOI" (Nov. 2017).

[6] *See supra* note 3.

and an operative-level competent authority agreement that governs the details of the exchanges. All jurisdictions have so far opted to use multilateral instruments: the Convention on Mutual Administrative Assistance in Tax Matters and the CRS Multilateral Competent Authority Agreement.

After establishing the legal framework, a jurisdiction must activate it in time for exchanges with all interested appropriate partners. The CRS multilateral agreement requires activation for each bilateral exchange relationship, which includes providing confirmation that the legislative, operational, and confidentiality requirements are in place.

Third, a participating jurisdiction must establish operational procedures and IT infrastructure that guarantee the integrity and confidentiality of information. That should enable it to both receive the information collected by financial institutions required to do so under the CRS and securely transmit that information to its exchange partners.

For transmitting information to exchange partners, all participating jurisdictions have decided to use the common transmission system put in place by the OECD's Forum on Tax Administration and managed by the Global Forum. Even so, participating jurisdictions must still have technical solutions for linking their information collection and transmission systems into the common transmission system.

Finally, all tax information exchange is subject to strict confidentiality and data safeguard obligations.[7] The OECD has developed a legal mechanism for ensuring security and confidentiality, and all jurisdictions must satisfy the safeguard requirements before exchange begins. To promote compliance by jurisdictions, the Global Forum conducts peer reviews. If the forum identifies gaps, a jurisdiction must put in place a plan of action for addressing them before it can receive information.

AEOI Challenges and Technology

In Africa, only Seychelles and South Africa took part in the first AEOI exchanges in 2017; Mauritius joined them in 2018. Ghana and Nigeria are committed to begin first exchanges in 2019, while Morocco and Egypt are partnering with France and the United Kingdom, respectively, under pilot projects facilitated by the global forum.[8] Africa is composed of 54 countries, 29 of which are members of the global forum, making it disproportionately underrepresented in the AEOI process.

AEOI is heavily dependent on technological, computing, and administrative capacity, which may be lacking or weak in many African countries. Therefore, there is a potential for technology at several points in the AEOI process to help African countries fast-track their participation and reap the benefits associated with greater transparency.

Domestic Treatment of Information

The information on financial accounts to be exchanged under AEOI is first collected by financial institutions. It is then sent to the institutions' domestic tax authority, which sorts it out and makes it ready for automatic exchange with the tax authorities where the account holders are residents. Because exchange is reciprocal, African countries will not be able to access AEOI unless and until they demonstrate capabilities for collecting the information required for exchange. That calls for close coordination between the reporting financial institutions and tax authorities with an established process for collection and relay of the information from the financial institutions to the tax authority,[9] as well as sound technical infrastructure for the successful collection, handling, and relay of the information from the financial institutions and the tax authority, while keeping the taxpayer data confidential and secure. In many developing countries, the technical infrastructure that

[7] *See, e.g.*, article 26(2) of the OECD Model Tax Convention on Income and on Capital; paras. 11-13 of the commentary to the OECD model convention; article 8 of the OECD model TIEA; and article 22 of the Convention on Mutual Administrative Assistance as amended by the 2010 protocol.

[8] *See* Global Forum, "Tax Transparency in Africa: Africa Initiative Progress Report 2018," 29, 31-32 (2019); and, "Implementation Report 2018," *supra* note 3.

[9] Christian von Haldenwang et al., "Tax Transparency and Exchange of Information (EOI): Priorities for Africa," T20 Argentina 2018 Task Force: Cooperation With Africa (July 25, 2018).

supports secure collection and relay may be lacking. Technology can play a role in making the collection, storage, and transmission seamless and secure.

Confidentiality and Safeguarding Data

To participate in AEOI, a jurisdiction must meet the relevant CRS technical standards and apply safeguards to protect taxpayer information. Data will not be sent to a jurisdiction until it receives a satisfactory global forum assessment of its confidentiality and data safeguards. That assessment is also important for country-by-country reporting and beneficial ownership information that relies on the same data and confidentiality safeguards. A jurisdiction's mechanism for information exchange should ensure the confidentiality of information received, which is not the case for many developing countries.[10] Those countries can access AEOI by deploying technology that enables them to meet the infrastructure deficit — that is, keep information confidential and secure. Technology can also help tax authorities determine who has access to the information received, trace personnel access, and maintain secure access logs.

Using Information Effectively

AEOI involves the transmission of bulk taxpayer information from foreign tax authorities. Many countries in Africa might have limited capability to receive, manage, store, and work with the different types of data received. If African tax authorities do not establish the necessary infrastructure to handle the data, they will not benefit from AEOI. They must invest in data analytics, risk identification systems, and auditing skills to ensure the information received is used effectively. That includes systems for identifying and matching resident taxpayers with information received under AEOI.[11]

How Digital Integrity Technology Can Help Africa

To best address the issues raised above, tax authorities must ensure that they comply with their obligations and standards and that taxpayers trust their technology functions. That is feasible with the help of digital integrity technologies, which are accessible, affordable, and relatively easy to implement. It is likely that each country will tailor technologies to those that best fit their domestic governance and rules, while satisfying international standards. The additional revenue gains from efficient AEOI will more than cover the cost of digital technologies.

As shown in Figure 1A, digital integrity technologies should foster trust in data, taxpayers, systems, and digital infrastructure. Data must be secure against hacking and leaks: The global forum's August suspension of Bulgaria's National Revenue Agency following the hacking of its database — including data exchanged as part of AEOI — is evidence of that point.

Data should be immutable, which implies that they cannot be tampered with,[12] and creating fake data should be impossible. Taxpayer data must be kept confidential, safe from unauthorized access, and be used exclusively for tax purposes. Only necessary data should be transferred and accessed.

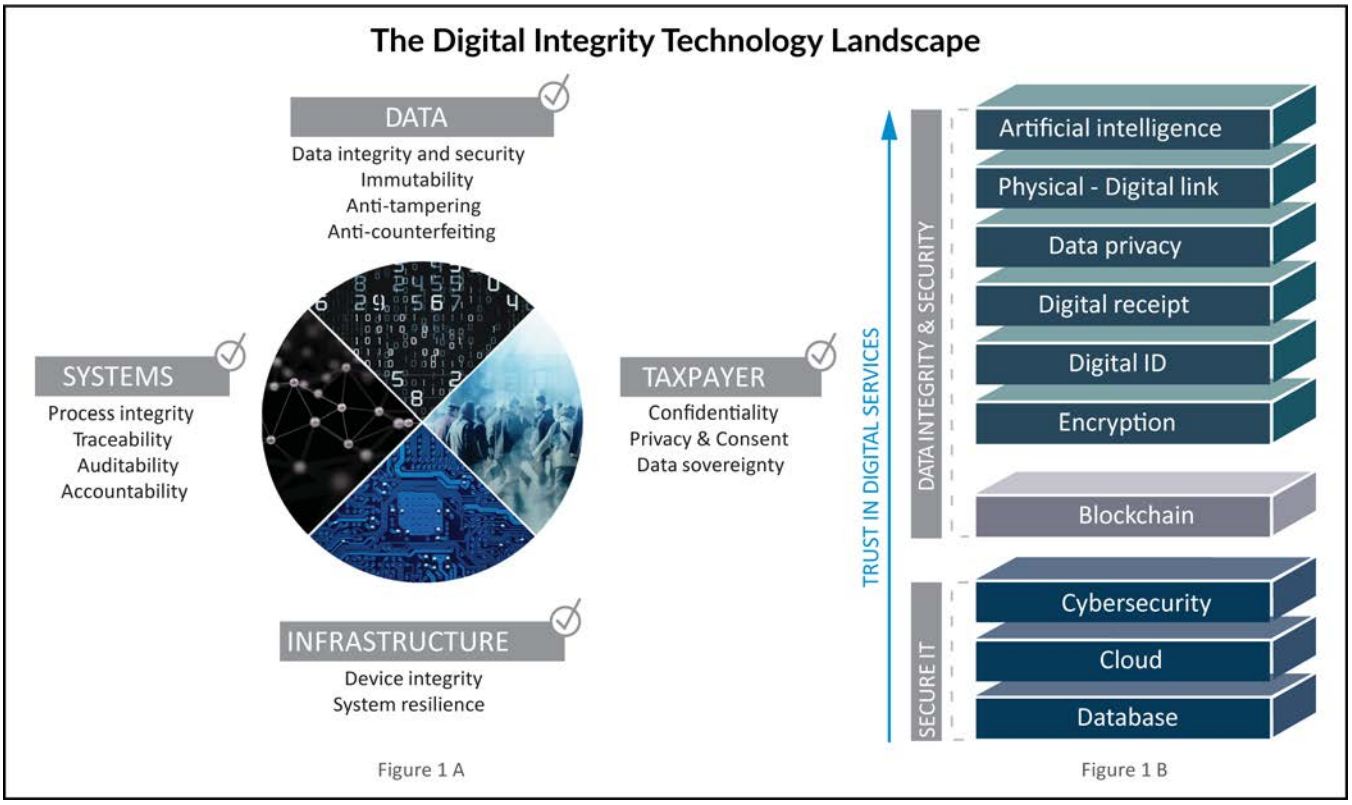
The taxpayer can digitally give his consent to data access and even data visualization by other actors. The systems should allow every transaction, including those by the original data creator, to be traceable, which will strengthen actor accountability. The data should be auditable, but only by authorized people (and like data, access logs should be protected against tampering and counterfeiting). Further, the integrity of the data process should be guaranteed. Finally, the digital infrastructure (both hardware and software) should be fully functional as required, protected against malicious interference, and highly resilient.

Digital integrity solutions for achieving the goals described in Figure 1A are already available. An array of technologies can be efficiently bundled as a secure e-registry accessible by all concerned parties. That e-registry is based on a technology stack (see Figure 1B).

[10] *See, e.g.*, *supra* notes 3 and 5; and Global Forum, "Tax Transparency in Africa," *supra* note 8.

[11] Haldenwang et al., *supra* note 9, at 8.

[12] *See* Global Forum, "Statement on the Data Breach in the National Revenue Agency of Bulgaria" (Aug. 30, 2019).



First is the basic stage of digitalization, in which documents such as bank records and tax registries are put into databases. Next, and to facilitate data exchange, data should be stored in a cloud (either public or private, depending on a country's legal obligations and preferences). Advantages and limitations must be carefully assessed. Third, databases and clouds must be protected by state-of-the-art cybersecurity packages.

Several African countries already use those first three standard technology blocks.

The next step is to introduce blockchain technology, which acts as a trust anchor, to ensure the immutability of data and transactions.

AEOI and EOI require the transmission of data, making it crucial to ensure that data are encrypted using strong cryptography. It is also important to use efficient methods to safeguard and protect the encryption keys. Next, a secure digital identity should be used to simplify the digital signature of any digital action.[13] That digital ID could initially be limited to a small universe that includes the tax authority, financial institutions, and actors involved in handling the data for AEOI and EOIR. The record of digital transactions should be made available in the form of a digital receipt. That is proof of a transaction, independent from the system.

As noted, special care should be taken to guarantee data privacy and ownership. In many countries, data protection laws are bound to become more stringent, with an increased role for technology. One leading example is the EU General Data Protection Regulation. Guidance for African countries can also come from the core principles for data protection developed by the U.N. Conference on Trade and Development.[14]

It could be useful to establish a digital-physical link in case a digital transaction is associated with a physical asset or to ensure that the right person stands behind a given identity. Finally, artificial intelligence and data analytics can be used by tax authorities to better examine

[13] Adopting and propagating digital identities and signatures are supported, for example, by the U.N. Broadband Commission for Sustainable Development and the World Bank's Identification for Development.

[14] *See* UNCTAD, "Data Protection Regulations and International Data Flows: Implications for Trade and Development," UNCTAD/WEB/DTL/STICT/2016/1/iPub (2016).

data, identify risks, and target audits. Those are likely to be useful for African countries as recipients of information.

Blockchain Technology

As mentioned, blockchain acts as the trust anchor. To build a high level of trust in digital services — especially for sensitive tax information — blockchain is necessary but insufficient. It is essential to make use of the aggregation of different technology bricks shown in Figure 1B. Countries mainly rely on the secure IT technologies (databases, cloud, cybersecurity) for EOIR and AEOI; to our knowledge, none use blockchain.

Not all types of blockchain are likely to be appropriate for AEOI and EOIR. Indeed, African tax authorities will have to continually collect, manage, and transfer large amounts of digital information. That means the blockchain must be both agile enough to easily and efficiently secure large amounts of data (scalable) and managed collectively under the authority's guidance (trustworthy).

In that context, both traditional public and private blockchains have major limitations,[15] although not all blockchains share those features. For instance, the KSI® Blockchain used by Estonia since 2008[16] solves the scalability and trust concerns of most public and private blockchains. It is akin to a private blockchain infrastructure publicly exposed, and protects large quantities of data in a range of fields, including medical, legal, and judicial, as well as from financial institutions and banks.[17]

The KSI® Blockchain is used to secure the integrity of billions of digital objects per second.[18] Every object registered on the blockchain — from a single log line to a full disk image — generates a proof of inclusion for signing time, integrity, and the signer's identity that can be instantaneously and independently verified. That real-time scalability is important in AEOI, because it can help securely record a change in things such as the holding of assets or in parties' level of control. Any change to blockchain-registered records can be made immediately evident.

Blockchain solutions should be designed to be implemented on top of existing infrastructure. The KSI® Blockchain, for instance, can be integrated into government and financial sector infrastructure and does not require data to be migrated from legacy systems. Blockchains such as KSI® are also superior to alternative, non-blockchain forms of ensuring data and process integrity. In contrast to blockchain, legacy technologies do not scale easily to cover the billions of digital objects whose integrity must be assured. Further, legacy technologies require trust in a third party, which may not exist across borders, and create additional long-term complexities.

Integrity of the Process

Beyond data integrity, technology should also ensure that data have been generated via the right process. For AEOI, a correct process might entail the proper sequencing of transactions or the association between a single transaction and a generic contract. If a transaction is secured by the KSI® Blockchain, events such as wrong sequencing or attempts to backdate documents will be blocked. Further, to prevent an individual from introducing in the blockchain several valid generic contracts and extracting the most favorable contract at year-end, the process will ensure the individual can record only one contract. The quality of securely timestamping events in the blockchain addresses fraud, such as backdating transactions and creating fake transactions.

Artificial Intelligence

Data received by African tax authorities under AEOI must be processed and evaluated to provide meaningful additional tax revenue. Processing and evaluation can be accomplished

[15] Public blockchains suffer from scalability, performance, and privacy concerns and lack compatibility with legacy systems or agreements for service level. Private blockchains build a trust model on consensus among computers hosted by participants in a closed network, but rely on trust in that network and create an ongoing expense of maintaining it.

[16] Estonia started its first pilot implementation of the KSI® Blockchain in 2008 and put it into operation in 2012. The same technology is also used outside Estonia to ensure physical and data supply chains in a range of industries.

[17] IMF, "Fiscal Monitor April 2018 — Capitalizing on Good Times," at 76-77 (2018).

[18] The theoretical scalability of the KSI® Blockchain is 1,000 billion objects per second (10^{12}). For comparison, the bitcoin blockchain can address only a few transactions per second.

using artificial intelligence, whose key contribution is to help strengthen risk analysis of taxpayer profiles and transactions, thus better targeting enforcement. Indeed, artificial intelligence can be set up so that it points to risky transactions based on selected characteristics of misbehavior or on statistically outlying values compared with standard figures, averages, or predetermined thresholds.

Summary

Digital integrity technologies can play a key role in helping African countries meet the requirements for AEOI participation. They can enable the secure gathering, storage, and management of information collected domestically, while maintaining its confidentiality. They can ensure the appropriate exchange of financial data among tax authorities and demonstrate the capability by African tax authorities to handle data received. Further, African tax authorities can use digital integrity technologies to make sense of data received, so that they can generate the proper level of tax revenue. The technologies are set up to provide the necessary proofs of digital integrity, enabling "trust by design" for all participants in the AEOI. Adopting them will allow developing countries to leap-frog more advanced countries. ■