



# USE CASE 3 **TAX RECORDS**

A Use Case and Issue Brief  
Prepared by CIPIT



**Strathmore University**

*Centre for Intellectual Property and  
Information Technology Law*

## BACKGROUND

Every state needs to raise revenue to fulfill its functions. Digitisation of tax records is an attractive proposition for states as they are able to track persons as they engage with government and private actors and then estimate expected tax.

Many African countries that took loans from China in the past decade are increasingly seeking ways of expanding the tax net in order to increase revenue needed to repay the maturing loans. Digital Identity (DID) aids this by providing the state with general information on taxpayers which can be used for ensuring taxpayers pay appropriate amounts and on time. With the advent of big data analytics, countries such as Kenya and Uganda have also been gaining insights from DID data to predict expected taxes from various categories of taxpayers.

The nature of taxation, together with the power that tax authorities wield, means that tax records are a functional ID system with aspects of a foundational ID system. This is because tax records are linked to many other functional databases. For example, in countries where taxation is on the basis of self-assessment, one is required to file a variety of documents (e.g., insurance claims or work-related invoices) to support their self-assessment.

To enhance registration for taxation, many countries make it mandatory to register as a taxpayer in order to receive other services. For example, one needs a tax ID in order to receive employment income. This links employment data with the tax database.

### **JUSTIFICATIONS FOR THE USE CASE**

Digital ID is implemented by a tax authority for reasons such as:

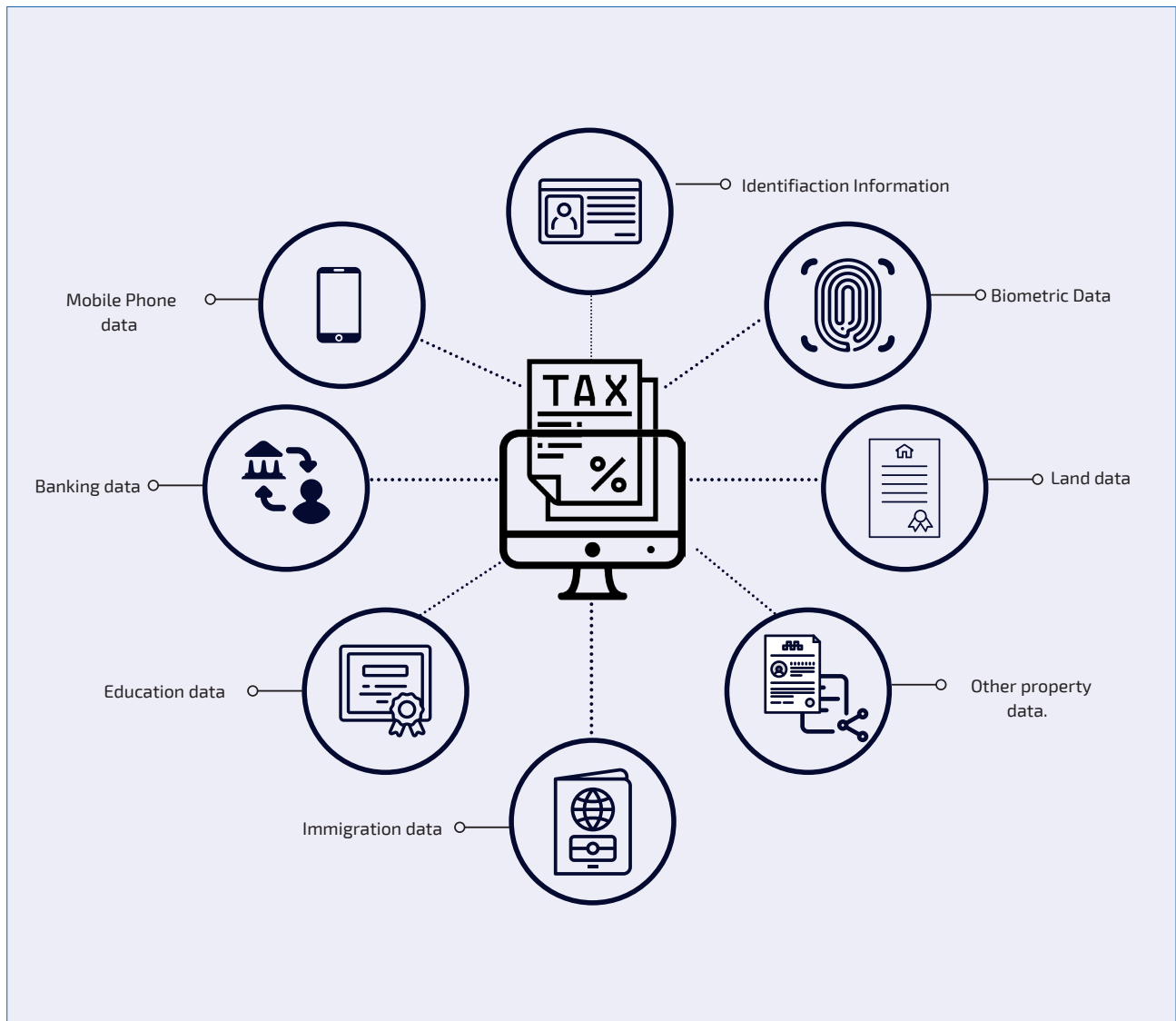
1. Increase the tax net by registering everyone who is a potential taxpayer
2. Increase efficiency through automation of services such as tax payments and tax clearance certificates
3. Extract data on national public finance
4. Fairer distribution of national burden by ensuring more people pay taxes

### **DATA INVOLVED IN THE USE CASE**

Depending on the rules, digital tax ID can collect very broad data or be linked to a wide range of data such as:

1. Identification information (foundational ID information, also family relations, etc.)
2. Biometric data for verification
3. Land data for property taxes
4. Other property data e.g motor vehicles, company shares
5. Immigration data where tax ID is required for passport
6. Education data where tax ID is required for college loans

- 7. Banking data
- 8. Mobile phone data
- 9. Credit history data



**RISKS INVOLVED IN THE USE CASE**

The risks associated with digital tax ID include:

1. Probability of tax officials back-linking to other ID for tax assessment
2. Disclosure of highly sensitive financial data during tax investigations
3. Unwarranted linking of individuals due to inaccurate data
4. Prejudice from automated decisions
5. Loss of highly sensitive financial data about individuals
6. Use of the data by government for purposes that are not consistent with human rights norms

## ANALYSIS

Tax digital ID is controversial. While on the one hand it has potential to increase revenue collection and subsequently service delivery, tax authorities in many countries often overstep in their search for data for tax assessment, leading to violations of the right to privacy. In Kenya for example, the tax authority sought to analyse mobile money data in order to assess taxes. While this was resisted, the authority assessed some state agencies data, e.g., the Higher Education Loans Board and Kenya Power Company records, to relate their data against taxpayer returns. In return, the state agencies also get data from the tax agency, which has sometimes been used to make decisions that have legal effect, as explained in the case study below.

The requirement for tax ID in order to access other government services is also unfair to the extent that sufficient information is not given to the registered tax payers on their obligations on attaining the tax ID. Many acquire it as a formality without understanding the tax obligations they have been registered for. They thereafter find that they have been fined for not fulfilling those obligations.

It is also potentially inappropriate when tax authorities access other identity databases for tax assessment without the knowledge of the data subject. This may be further compounded by inaccuracies in the different databases. For example, land transfer processes may be complex, involving updates to numerous databases to complete the transfer process. It is not unusual for updates to some systems (e.g., utility company databases) to fail to take place or to be substantially delayed. In such cases, and where the property and other databases are interlinked with tax records, prior owners may become the target of improper tax assessments.

Given that tax authorities have wide ranging powers such as search and seizure, freezing of assets, criminal prosecution and imposition of fines, there should be very clear rules on when and how they can access digital ID databases linked to tax ID. In addition, there should be caution in the use of automated decision-making processes linked to tax DID to avoid unfair administrative action. Further, every taxpayer should be able to know how their data is being used by either the tax authority or other agencies linked to or using the digitised tax ID.



### GOOD ID PRINCIPLES IN THE USE CASE

1. Careful consideration of purpose when defining any digital ID that may be linked to tax ID
2. Independent oversight of use of tax ID and any linked digital IDs
3. Good governance to avoid misuse of the privilege of access where there is sharing of data between tax authority and other institutions
4. Protection of the rights of taxpayers, including the right to access their data
5. Responsive complaints procedures for those who may be aggrieved by tax ID decisions
6. Multiple strong checks on the use of data by data processors. Such checks include a functioning judiciary, government oversight committees, and strong civil society organizations.
7. Respect for the rule of law.
8. A data protection legal regime that specifically lists financial data as highly sensitive data.
9. Mandatory encryption of data, and mandatory use of PKI.

## CONCLUSION

The risk of inappropriate use of digitised tax ID data is extremely high, but the use of any alternatives is inconceivable. There should be well thought out principles on use of DID with respect to tax collection, with well-defined cases of when and how data may be shared between tax authorities and other agencies.

## ADDENDUM: KENYA AS A CASE STUDY.

The Kenya Revenue Authority (KRA) initiated the real estate strategy in 2016 where among others, they aimed to increase collection of rental income. In 2018, they sought to assess taxes due from small landlords including those providing informal settlements. KRA analysed data from the state power monopoly, the Kenya Power Company and isolated those who had multiple electricity meters registered in their names. Such people were assessed against their previous year's tax returns.

KRA used identification by attribution in the analysis. Attribution involves collecting attributes that collectively identify an entity. Attributes that were used to identify landlords included multiple utility bills and average amount of power consumed. KRA assumed that all those with multiple utility bills and moderately high power bills were landlords. Many who were presumed to be landlords were then called over the telephone then interrogated about their tax returns. It turned out that many of those who provide informal settlements are also not digitally literate and do not understand the substantive aspects of filing taxes. They normally use cybercafes (intermediaries) to file their tax returns. Cybercafes mostly file nil returns.

During the tax returns filing period last year, KRA set up tents in town centres with informal settlements to assist landlords in those areas to file returns. Many of the landlords who are not digitally literate did not distinguish this exercise from their usual filing of returns at the cybercafe, save for the fact that instead of paying at the cyber, they used mobile money to pay KRA. This shows the need for public education and digital literacy in digitalisation projects.

KRA still plans to relate its data with other data, such as banking and mobile phone data to assess taxes on more landlords. This will, it is claimed, improve attribution by identifying patterns in financial income that suggest rental income. In the 2018 Finance Act, banks and financial institutions were instructed to collect KRA Personal Identification Numbers (PIN) from all their customers. KRA provides an online PIN verification service.

### CONCERNS

The tax authority is allowed by law to access information to enable it to assess the amounts due to the government in taxes. However, the right to privacy, including data protection, is constitutionally and legally guaranteed, and any limitation should be legal, proportional and necessary. The arbitrary nature of the real estate strategy means that it may fail the proportionality and legality requirement. The right to access information should not infringe other constitutionally guaranteed rights.

One of the taxation principles is clarity: i.e., the tax laws should be comprehensible to the taxpayer. The aim of this is to avoid arbitrary administration of taxes. Whereas it is necessary and legally sound for the tax authority to access electronic data in order to recover unpaid sums, the process should be guided by law and not result in an unjust result. The process should be clear on what avenues will be used, and the deductions and rights to which the taxpayer is entitled by law.

In this case, the taxpayer is not aware of the fact that personal information they have shared with Kenya Power Company is shared with third parties such as KRA. The current Data Protection Act allows the collection of data from a third-party source if it is necessary for the enforcement of a law which imposes a pecuniary penalty. Avoidance of tax does incur a penalty. KRA can enforce the recovery of unpaid tax by accessing records held by a financial institution or public authority, with

---

the aim of assessing taxes . The entity holding this information is however required to notify the data subject of the 3rd party to whom the personal data has been transferred .

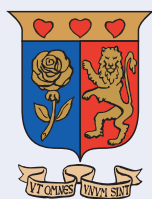
In addition, inaccuracies in the Kenya Power database have resulted in some people being attributed as landlords while in fact they are not. This is the case with those who transferred land but the buyer did not update the Kenya Power database, as well as those who may have been registered for meters with Kenya Power without their knowledge. However, KRA assumes that the Kenya Power database is accurate when carrying out the database relation exercise.

#### **CONCLUSION**

KRA duties to collect revenue are definitely improving from digitisation. KRA was among the first public entities to digitize records and systems, and they have therefore had the benefit of testing their systems for a longer period. They are aware of the need for more data for big data analytics, hence the strategy to access other public databases, such as Kenya Power.

However, all state power must be exercised in a constitutionally sound manner that protects and upholds the rights of people. KRA's data work should therefore be assessed against data protection principles so as to balance its need for further revenue collection with every person's rights to privacy. This includes, but is not limited, to carrying out a data protection impact assessment for all activities carried out by KRA.





Ole Sangale Rd, Madaraka Estate.  
PO Box 59857 00200, Nairobi, Kenya | Tel +254 (0)703 034 612  
Email: [cipit@strathmore.edu](mailto:cipit@strathmore.edu) | Website: <https://cipit.strathmore.edu>