IDENTIFICATION FOR DEVELOPMENT

# ID4D Country Diagnostic: Ethiopia

WORLD BANK GROUP

Cover photos: Top left by Daniel Silva; top right by Natalia Cieslik/World Bank; bottom by Binyam Teshome/World Bank.

# Contents



**Figures and boxes**

# About ID4D

The World Bank Group's Identification for Development (ID4D) initiative uses global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems to achieve the Sustainable Development Goals. It operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, and legal, among others.

The mission of ID4D is to enable all people to access services and exercise their rights, by increasing the number of people who have an official form of identification. ID4D makes this happen through its three pillars of work: thought leadership and analytics to generate evidence and fill knowledge gaps; global platforms and convening to amplify good practices, collaborate, and raise awareness; and country and regional engagement to provide financial and technical assistance for the implementation of robust, inclusive, and responsible digital identification systems that are integrated with civil registration.

The work of ID4D is made possible with support from World Bank Group, Bill & Melinda Gates Foundation, and Omidyar Network.

To find out more about ID4D, visit worldbank.org/id4d.

# Acknowledgments

This report was produced June 2017 by Alan Gelb (consultant) and Robert Palacios (Global Lead, Pensions and Social Insurance, World Bank) at the request of the Government of Ethiopia as part of a broader technical assistance engagement on Civil Registration and Vital Statistics (CRVS). This work is financed under the Rapid Social Response (RSR) Trust Fund managed by the Social Protection and Labor Global Practice at the World Bank. The authors would like to thank the many government officials interviewed for their time and patience.

# Abbreviations

| | |
|---|---|
| AFIS | Automated Fingerprint Identification System |
| CBHI | Community-based health insurance |
| CRVS | Civil Registration and Vital Statistics |
| EPRDF | Ethiopian People's Revolutionary Democratic Front |
| FDRE | Federal Democratic Republic of Ethiopia |
| INSA | Internal Security Agency |
| KYC | Know Your Customer |
| MoH | Ministry of Health |
| MoJ | Ministry of Justice |
| MOUDC | Ministry of Urban Development and Construction |
| NID | National Identity |
| PSNP | Productive Safety Nets Program |
| RVERA | Regional Vital Events Registration Agency |
| VERA | Vital Events Registration Agency |

# Executive summary

This report documents the most important types of identification that are currently being used, as well as the new system that is being planned in Ethiopia and the legal and institutional context in which they exist. It is a somewhat unique case in that the most important form of identification is the kebele ID card which is issued by local administrators in more than 16,000 different locales. The kebele card confers legal identity. It allows individuals to directly or indirectly (by providing sufficient proof to obtain a different form of identification) to conduct almost any public or private transaction, including obtaining a passport or voting in an election. Moreover, it is very accessible and based on anecdotal evidence; most Ethiopian adults have one. In many ways, it functions as the de facto national ID yet there is no central registry, no way to ensure uniqueness, and an extremely weak credential that can be easily faked. Recent legislation replacing this system with a new, modern national ID has not been implemented more than four years after its passage.

Births and deaths are also recorded at the kebele level where in most cases, a list of children along with other members of each household is maintained in ledgers. The number of births (and deaths) is reported by each kebele to the state government which monitors what are the equivalent of vital statistics. These functions would, in most countries, be performed by the civil registry. However, this institution, known in Ethiopia as the Vital Events Registration Agency (VERA), was only established in 2014. It began to issue birth and death certificates and record other vital events in August 2016.

In short, the Ethiopian identification system is in transition. It is in the process of moving from a highly decentralized system that functioned reasonably well in a predominantly rural environment with limited migration, to a modern system of civil registration and, eventually, a national ID based on biometrically determined uniqueness and a secure credential. Ideally, these two elements of Ethiopia's identification system would be linked through the issuance at birth of a unique number to be applied when the child becomes an adult. This report describes the many challenges that Ethiopia's government will have to overcome along with some possible solutions as its new identification system is born.

# 1. Introduction

Ethiopia's system of identification is at a crossroads. For the first time, a proclamation issued in 2012 establishes two new government agencies tasked with the implementation and management of a civil registry and a national ID. Implementation began in August, 2016.[1]

As discussed below, Ethiopia is an atypical case in that most of the adult population already have a form of identification that allows them to identify and authenticate themselves for a variety of purposes ranging from opening a bank account to getting a passport. Also, most children are now listed in books kept at the kebele level and are being issued certificates that are required to attend school. So, unlike many countries at a similar income level, Ethiopia's identification challenge is not accessibility or coverage.

Instead, the need to improve the way Ethiopians are identified derives from the low quality of the existing forms of identification which cannot ensure that an individual cannot claim multiple identities. Nor is the current credential (the card) a secure way of proving identity to a third party, a deficiency compounded by the lack of a central registry. Instead, the files related to identification are on paper and kept at the more than 16,000 kebeles around the country. This makes them almost impossible to use for anything beyond local administrative purposes and will become even less useful as the population continues to migrate from rural to urban areas.

This report aims to provide a holistic analysis of the current and emerging system and to provide options to be considered for meeting the challenges of building a new identification system. The next section reviews the legal and institutional context for Ethiopia's recently legislated identification system. Section 3 lays out the findings of the analysis and describes the identification ecosystem, including the existing forms of identification that the new system will replace. Several 'functional' registries are also reviewed. The final section reviews options for addressing the challenges that the two new agencies will be facing in a very short time.

1 The original schedule called for implementation to begin on July 1, 2015, but this was subsequently amended to allow more time for preparation.

# 2. Legal and institutional context

This section reviews the legal and institutional context which has recently emerged due to legislation passed in 2012. No. 760/2012: "A Proclamation on the Registration of Vital Events and National Identity Card." Section 2.1 deals with Civil Registration and Section 2.2 with the NID. The first, the Vital Events Registration Agency, is responsible for civil registration and vital events. In addition to the federal level agency, regional vital events registration agencies or RVERAs are established in each of Ethiopia's nine regions. The second, the National ID Agency, is responsible for enrolling all Ethiopians over the age of 17 into a national database and issuing to them a national ID card. The two forms of identification implied by this proclamation—the birth certificate and the national ID—are to be linked with a unique national ID number to be issued by the NIDA and included in the birth certificate issued by VERA. The starting date for the implementation of this new system was originally set as July 1, 2016.

## 2.1 The Vital Events Registration Agency (VERA)

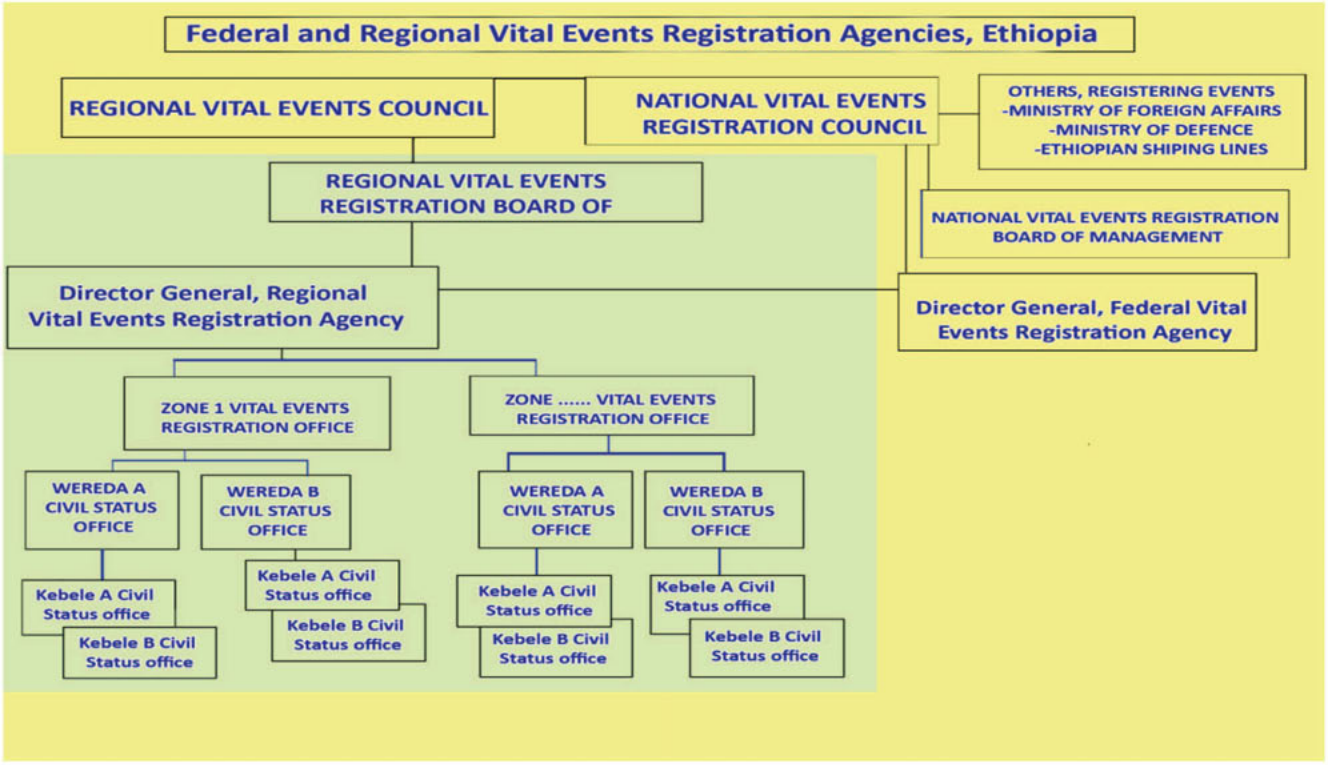
The Civil Registry in Ethiopia is among the youngest in the world having been established by law in August 2012. The original legislation relating to civil registration dates back to 1960 in the form of Ethiopia's Civil Code. However, the relevant provisions were never activated. It was not until the Family Act in 2000 that marriages and divorces that had been issued by municipalities and towns were underpinned by legislation. Finally, in August 2012, the Federal Democratic Republic of Ethiopia (FDRE) issued the *Registration of Vital Events and National Identity Card Proclamation No. 760/2012* covering registrations and vital events in Ethiopia (Federal Negarit Gazeta, 2012). This law repealed Articles 47 to 153 of the 1960 Civil Code, which were provisions on civil registration that had been suspended indefinitely.

*Regulation No. 278/2012 to Provide for the Establishment of the Vital Events Registration Agency*, hereafter referred to as Regulation No. 278/2012, established the following national bodies in December 2012: (a) Vital Events Council; (b) Board of Management; and (c) The Vital Events Registration Agency (Federal Negarit Gazeta, 2012b). The Vital Events Council (articles 8 and 9) is the highest authority on matters of civil registration. It is chaired by the Minister of Justice with additional members designated by the government.[2] The Director General of the federal Vital Events Registration Agency is the secretary of the Council. The Board of Management provides oversight to VERA and members are also designated by government. VERA itself is ostensibly an autonomous agency mandated to direct, coordinate, and support the registration of vital events nationally, as well as to maintain records of these events. It falls under the Jurisdiction of the Ministry of Justice.

Ethiopia is a federated state with nine autonomous regions and two city administrations. It follows a decentralized administrative system where the regions have legislative, executive, and judicial powers. The organizational arrangement for vital events registration follows the decentralized administrative structure. As shown in Figure 1, the next organizational tier is at the regional level through the RVERA, reflecting Ethiopia's federal structure.

2 These include the following: Ministry of Justice (MoJ); Ministry of Finance and Economic Development (MoFED); Ministry of Health (MoH); Ministry of Education (MoE); Ministry of Urban Development and Construction (MoUDC); Ministry of Foreign Affairs; Ministry of Defense; National Intelligence and Security Service; Ministry of Women, Children and Youth; Ministry of Federal Affairs; Government Communications Affairs; and City Administration of Addis Ababa and Dire Dawa. At the time of writing, the Council was holding monthly meetings.

**Figure 1: VERA Organizational Plan**




*Source:* Towards sustainable vital events registration and vital statistics system of Ethiopia: Strategy and Action Plan, July 2013–2018.

# 2.2 The National ID Agency

The legal basis for the NID as well as for the establishment of a civil registration system is Proclamation No. 760/2012: "A Proclamation on the Registration of Vital Events and National Identity Card." The proclamation motivates the NID project by noting that: "the issuance of national identity cards to citizens has become important for the protection of national security, and for providing efficient services to citizens by the public and private sectors."

It states that the NID is to be managed by "an appropriate Federal Organ." Implementation was originally scheduled for July 1, 2016. However, unlike VERA, the agency has not been constituted since the necessary regulations have not been issued. It falls under the jurisdiction of the internal security agency, INSA. The director of INSA, which also has the responsibility for digital technology and cybersecurity, has the status of a minister and reports directly to the Prime Minister.

Registration is compulsory. Applicants are required to provide the following information:

**a.** full name including grandfather;[3]

**b.** special identification, if any;

**c.** parents' full name and citizenship;

**d.** date and place of birth;

3 The naming convention in Ethiopia follows a patronymic system similar to that used in Iceland. There are no surnames. Children are given a name at birth; this is followed by their father's first name and their grandfather's first name. The three names together constitute the complete name.

**e.** sex and marital status;

**f.** principal residence and occupation;

**g.** ethnic origin and religion;

**h.** photograph and finger print; and

**i.** other necessary information as may be determined by the appropriate federal organ.

The national ID card is valid for 10 years. They should have security features and be deduplicated (biometrically), and would include the following information:

**a.** full name including grandfather, sex, date and place of birth, principal residence, photograph, finger print and signature of the holder;

**b.** national identification number and identity card number;

**c.** issuance and expiry date.

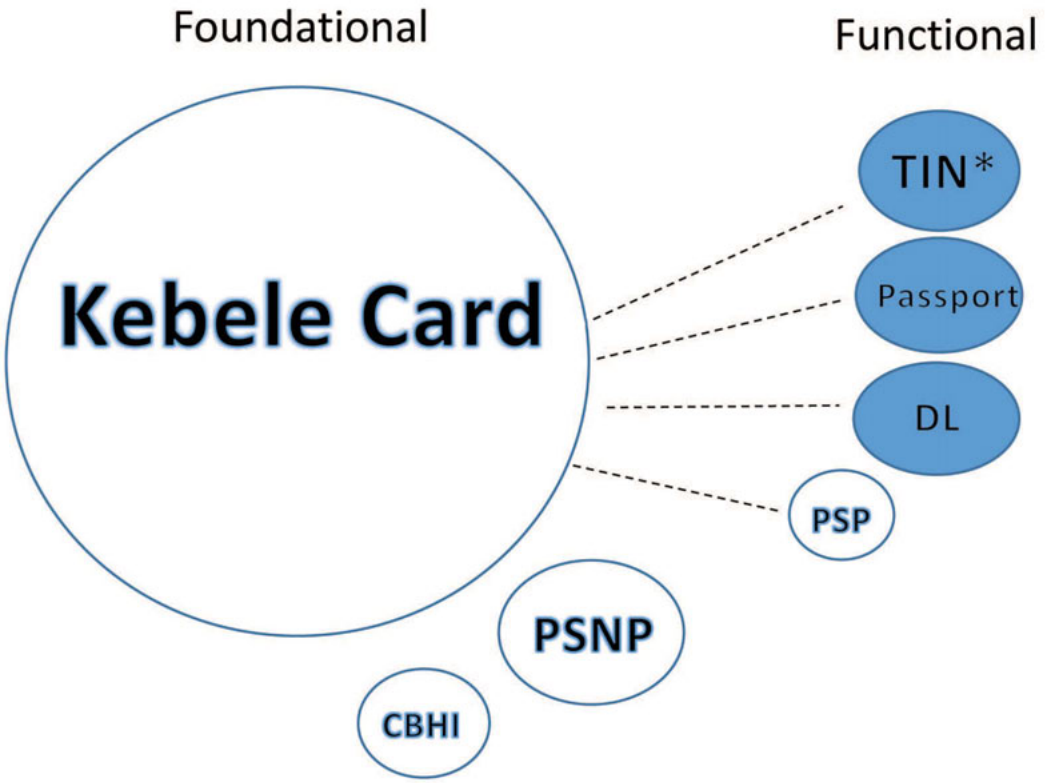
Holders are required to carry their cards and present them on official request. They should notify the authorities of any changes in their particulars within 15 days and present the card to the authorities for renewal upon the expiry of its validity period.

As discussed below, significant resources would be required to implement the plan for rolling out the national ID.

# 3. Description of the current ID ecosystem in Ethiopia

Figure 2 shows the major forms of identification used in Ethiopia. Using the terminology from Gelb and Clark (2013), the kebele ID would be considered a "foundational ID" while the others on the right are functional in the sense that they are forms of identification tied to a particular purpose or program. The size of the individual circles are meant to roughly illustrate the share of the population covered by each form of identification. While no official estimate exists, the widespread perception is that the vast majority of the adult population holds the kebele ID. The dotted line between the kebele ID and the four forms of identification indicates that they are obtained by presenting the kebele ID. The other functional forms of identification do not require it.

**Figure 2: Foundational and Functional IDs in Ethiopia**




Kebele card (? 40+ million)
TIN—Tax ID Number (2.2 million)
DL—Drivers' license (?)
PSNP—Cash transfer program (8 million)
CBHI—Community-based health insurance (0.7 million)
PSP—Public sector pension card (1.5 million)

*Notes:* (1) * = biometrically deduplicated, (2) White = paper or no credential; Blue = electronic credential

Clearly, the most important one is the kebele ID. This is a highly developed and pervasive paper-based system for the personal identification of adult Ethiopians, defined as individuals aged 18 years and above. This system is administered on a decentralized basis by Ethiopia's 16,475 kebeles, the lowest-level units of the administration. The kebele card is accepted and required for virtually all identification purposes—to register a SIM, open a financial account, travel internally, stay in a hotel, obtain a passport, and to enroll to vote. These forms of identification apply only to Ethiopian citizens. Foreigners and refugees are registered separately and have separate forms of identification. In some border areas, especially with pastoral populations, there have been disagreements over who should be entitled to an Ethiopian ID.

# 3.1 The kebele system and kebele card

Given the importance of the kebele card, it is useful to understand the nature of this administrative unit and its unique origin. Ethiopia is administratively structured into nine regions and two city administrations. In 2007, the regions and cities were further subdivided into 73 zones and these into 741 *woredas.* The *kebele* is the lowest form of administrative unit ('kebele'—Amharic for 'neighbourhood'). There are currently 16,475 kebeles, an average of 20 per woreda. Of the total, 1,618 kebeles are urban.

## The kebele system

The kebele system is one of neighborhood administration and control. Land reform was high on the political agenda of the Derg, which overthrew the monarchy of Haile Selassie in 1974. The imperial exploitation of the rural population was identified as one of the main reasons for national poverty and underdevelopment. In rural areas, peasant associations were assigned to redistribute land and persecute 'anti-revolutionary elements' with their own militias. The urban kebeles or revolutionary neighborhood associations were their urban equivalent (Treiber). Because of its functionality, the kebele structure was maintained after the defeat of the Derg and the accession of the Ethiopian People's Revolutionary Democratic Front (EPRDF) government in 1991 following a long period of conflict.

Kebeles are further subdivided into successively smaller entities: katanas, development groups, and down to the level of small neighborhood groups consisting of up to 5 households. As an example, one kebele in the woreda of Bosset consists of some 9,000 people. It is subdivided into 9 katanas, 97 development groups and 519 1–5 household groups. This structure serves to provide a tight connection between the kebele administration and the kebele households. With 85 percent of Ethiopia's population still living in rural areas and low, though increasing, internal migration, the composition of most kebeles has been relatively stable.

Every rural kebele and urban neighborhood kebele has its own kebele office. A typical kebele, with 5,000–12,000 residents, is administered by a "cabinet" elected by the residents. This may include four positions: Chairman, Deputy Chairman, Manager, and Development Officer. These will be assisted by a larger number of experts assigned by the government to the kebele: health agents, agricultural specialists, teachers, and natural-resource management specialists. Kebele officials carry out a wide range of functions. They may determine eligibility for food assistance, recommend referrals to secondary health care and schools (each woreda has at least one high school and these now have connectivity through the WOREDANET system), and help provide access to state-distributed resources such as seeds, fertilizers, credit, and other essential agricultural inputs. They run community social courts, local prisons, and, in some places, local militia that are used to maintain law and order. Registration of the adult population is one of their essential functions.

## Kebele registration

At the age of 18 a kebele resident is eligible to apply for a kebele card. While the exact procedures may differ from kebele to kebele, the process is always grounded in detailed personal knowledge of the applicant and the nature of her/his affiliation with the kebele. In one observed case, the applicant will have to complete a standard form, providing personal details and present this to the kebele manager together with two photographs. One is attached to the form and retained in the kebele's records, which hold information on all kebele families in separate files. The application may require supporting testimony from the relevant catana and/or development or neighborhood group. It must be approved by the chairman of the kebele. In another, less formal case that was observed, there is no standard form and the applicant is required to only present one photo. The application is verbal, but must be supported by a letter from the applicant's neighborhood committee. This is kept on file in the kebele's records. A typical kebele will issue ID cards on two or three days of the week, with around 20–50 cards issued on each of the days.

Kebeles accept a wide range of evidence to back up the information needed for the application. As evidence of age, birth or vaccination certificates provided by clinics or religious authorities are accepted. So are a kind of birth certificate issued by the kebeles themselves in response to requests—these require three witnesses. However, birth certificates are not requested frequently so that most applicants will not have any formal birth certificate. To indicate their age they can present school certificates for Grade 6 or for Grade 8 national examinations and possibly other evidence. Because of the central role of the kebele card, the local officials processing the applications constitute the *de facto* adjudicators of claims to Ethiopian nationality, though appeals are possible to higher levels of government.

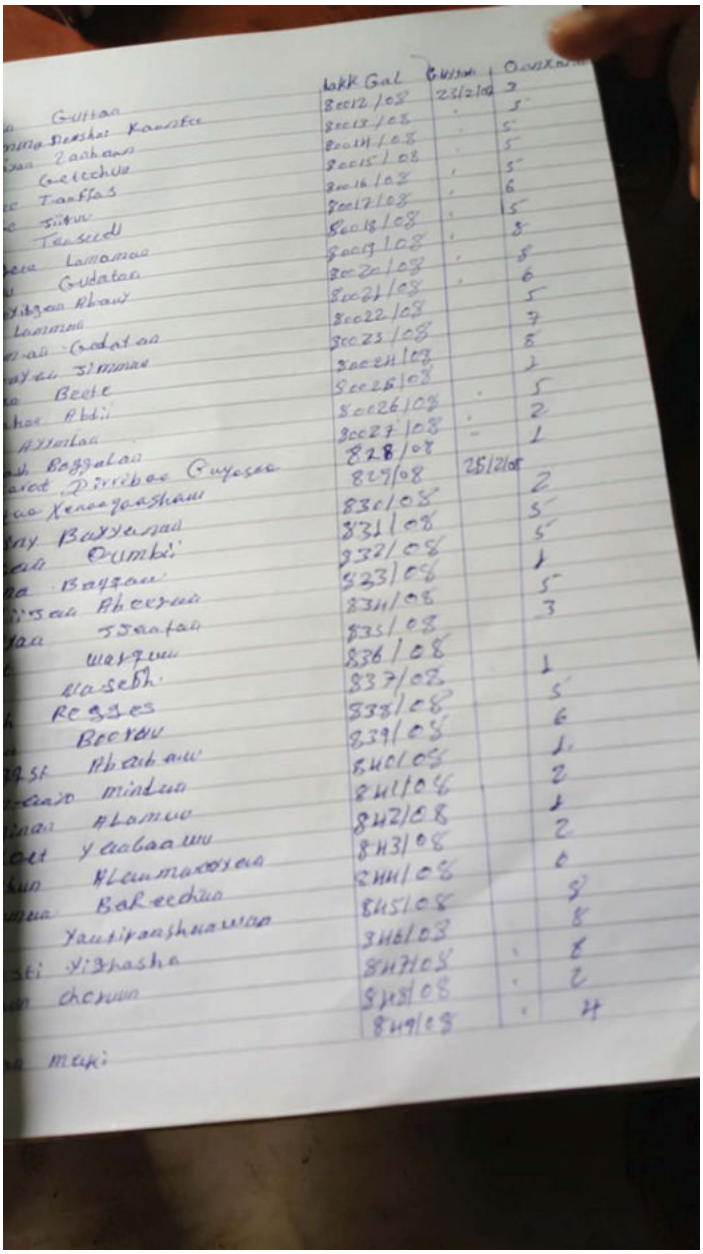
Kebele recordkeeping is very basic as are kebele office facilities. Files are kept in folders or bundles on open shelves as shown in Figure 3. They are vulnerable to fire, water damage, or simply deterioration. There are no backups. Although the kebeles provide summary information on the number and gender breakdown of their residents to their woredas every two years, the woreda does not hold records of the identities of the kebele residents.

**Figure 3: Kebele ID Records**

*Source:* Author's photo.

The details of recordkeeping vary between kebeles, even though they may be subject to oversight by the same woreda. Some kebeles maintain a sequential dated book entry of ID card numbers (see Figure 4) and the names of those to whom they have been issued. This provides an ongoing record of registered kebele adult members. Others do not maintain such a record, so that a query about a card issued to a particular member would require a painstaking search through piles of past letters and records.

**Figure 4: List of ID Card Numbers Issued**



*Source:* Authors' photo.

Kebele administrations keep no record of birth registrations or certificates issued. This may be done at the health post, which may issue a vaccination certificate at around nine months, after the completion of immunizations, to be presented on enrollment for school. The certificate supports evidence of birth but is an immunization, rather than a legally recognized birth certificate.

It should be recognized that this somewhat haphazard and variable set of paper registers is supplemented by the detailed knowledge of the kebele administrations and their sub- and sub-sub units. If the records of a kebele were destroyed, it would probably not be too difficult to reconstruct the details of kebele membership.

## The kebele card

Kebeles have a surprising degree of autonomy in the color and design of their kebele cards. They order cards from local printers in batches. Some are simple cards, with details of the applicant on the front and the stamp and signed authorization of the kebele on the reverse. Others are in the form of a folded booklet. Some come with card numbers pre-printed while others require the sequence number to be filled in by the kebele. Some cards are only in the local language. Others are also in Amharic and can be used directly to obtain a passport—no other documentation is required. Since national administration functions in Amharic, residents of kebeles that issue cards in only the local language must apply for a second type of card in two languages if they need this to obtain a passport.

**Figure 5: Variations in the Kebele Card**

*Source:* Authors' photos.

Kebele cards are valid for only a limited period but this too can vary. Some cards must be replaced with new ones every two years. Others can be used for four years but will need to be revalidated—in-person, at the kebele—every year. When cards are replaced, the number carries through so that each person has a unique kebele card number that remains unchanged as long as he or she remains a resident of that kebele. It seems that deaths are rarely reported, so that kebele cards lapse rather than being turned in when the holder expires.

While they may look different, kebele cards include a standard set of information: full name (including grandfather), mother's name, photo, data of birth, occupation, ethnic group, emergency contact details, kebele, woreda, date of issue, issuing officer, and kebele stamp.

Cards also include the telephone number of the kebele to facilitate queries on the authenticity of the document. Kebele IDs would be relatively easy to fabricate or alter, and there are reports that they can be readily obtained on the black market. However, on the basis of kebeles visited, such calls seem to be very rare. This suggests either that the incidence of fraudulent documents is very low or, more likely, that documents are widely accepted on face appearance without checking against kebele records. Indeed, the standard of recordkeeping in some kebeles would not easily support such checking which would require matching the name and ID number on the card to kebele records and also checking to see whether the photograph on the card corresponded to the one held on file.

Not all kebeles make it obligatory for every kebele member to hold a valid card although even in these they are held by a high percentage of the adult population. In one recent exercise that required the registration of all kebele residents for food aid, only about 5 percent were found not to have cards. Kebele administrations are tolerant of residents who do not hold valid cards and accept that they will only apply for cards when they need them. Cards are not free. Applicants are charged a fee, typically 10–20 birr, to defray the costs of printing the card. They will also need to pay for the photographs—typically 20 birr for 4 prints—as well as to travel to the nearest town or village with a photographer. With the minimum public-sector wage around 500 birr per month—and far lower incomes for most rural residents—the cost of obtaining a kebele card is not negligible. The cost of a kebele ID would be equivalent to about one-fifth of the monthly earnings of

beneficiaries of the Productive Safety Nets Program (PNSP) targeted at the rural poor. However, practice is not uniform. Some kebeles do require residents to hold an ID card but makes it available at no charge.

In principle, an individual can have only one kebele card at a time. Temporary absence from a kebele, for example, migration to Addis Ababa for seasonal work in the construction industry, can be accommodated through a temporary residence permit. Two years of residence or the intention to move permanently to a new kebele requires the resident to complete a form that includes the details of all family members migrating to the new destination. This is then submitted to the original kebele, together with kebele IDs that are then cancelled. The administration then issues a reference letter to the new kebele that serves as a substitute ID until the family has taken up formal residence in the new kebele. At that point a new ID with a new number is issued.

However, it is reported that in practice this system does not work seamlessly, and that individuals who do not go through the exit process with their existing kebeles are still able to obtain new kebele documents in various ways, including through family members who may be residents in different kebeles. Certainly, based on the limited number of kebeles visited, the incidence of exit applications appears to be very low. Some administrators who had been in their posts for several years reported that they had never been required to process an exit. While this could be due to genuinely limited mobility (in the sense of changes in permanent residence) or to a breakdown in the mechanisms to coordinate exits and entries across communities, widespread concern over multiple identities suggests that the latter is more likely.

## Strengths and weaknesses of the kebele ID

Relative to the situation prevailing in other low-income countries, Ethiopia's kebele ID system has some notable strengths. These reflect the features of its tight community-based administrative structure. To begin with, every adult "belongs" in a community, and has access to an ID credential issued by that community that serves virtually the full range of functions expected from an ID.[4] Obtaining a kebele ID involves relatively little transaction costs given its local administration.[5] ***Coverage is therefore very high***, although the charge for the ID and photos will be a disincentive for some poor people.

***The ID system is also integrated*** around the kebele ID. No other ID is required, for example, to obtain a passport. While a functional TIN is required, in addition to a kebele card, to open a bank account the TIN is derivative of the kebele ID. Similarly, the voter ID is a direct offspring of the kebele ID.

Ethiopia's tight community structure also mitigates the potential weakness of the kebele ID system in not being based on a working system of birth and civil registration. In more fluid or anonymous situations, early birth registration and certification forms the "breeder" process for national identification—the certification as to the origins of the individual concerned. Lacking sound continuous civil registration, some countries face difficulties to construct and maintain their population registers and ID baselines. They need to rely on special registration drives and similar processes to discover their adult populations and sometimes cannot be sure about their identities. With stable communities and administrative structures, the scope for possible ambiguities about the identities of Ethiopia's 18 year olds is reduced.

## Weaknesses

The kebele ID has quality limitations that will become more problematic with the development of its economy and society, as well as with the increasing use of Information and Communication Technology (ICT). ***The credentials issued by the kebele system are clearly vulnerable to forgery and alteration.*** Kebele-level registers are not always of sufficient quality to easily authenticate credentials.

4 As noted above, some groups might have more difficulty in establishing their claim to an Ethiopian ID than others, especially in border areas. This problem was not evident in the kebeles visited.

5 One kebele administrator interviewed said that it could be issued on the spot as long as the preprinted IDs were in stock.

***The kebele ID is also not deduplicated***. While ID cards may be unique within each kebele, there are no mechanisms that guarantee that identities are unique (deduplicated) across the country. Interviews suggest that it is not uncommon for individuals to have more than one kebele ID, especially in urban areas, although there are no good estimates of prevalence.

***Identity is not continuous over time***. Even if an individual has only one kebele ID at a time, he or she can have more than one kebele registration and number unless continually resident in a single kebele.

In light of these weaknesses, the kebele system is therefore increasingly challenged to provide for the identification needs of Ethiopia. The challenges will grow as Ethiopia develops, its population urbanizes and becomes more mobile, and moves further away from traditional social and communal structures. Ethiopia may not face some of the urgent needs that have driven ID reforms and new ID programs in some countries, such as massive payroll or benefit fraud. Some of the problems seen in other countries have been managed through extensive use of manpower. With a disciplined administration, personal visits can ensure that beneficiaries receiving cash-based transfers are living. However, the country will need to look ahead to different underlying conditions when considering future approaches toward the identification of its population.

## 3.2 Functional IDs

*Tax Identification Number (TIN).* These limitations have already resulted in the need to introduce the taxpayer TIN certificate and number to better secure identities for Ethiopia's formal sector and for clients of its banking system. It has been issued by the Revenue Authority since 2009. This biometrically de-duplicated certificate and number is held by around 2.2 million people.[6] It is required to open bank accounts (not mobile M-Birr or microfinance institution (MFI) accounts), for government employees, and for students who participate in public loans programs. The TIN requires the presentation of a kebele ID as do almost all other forms of ID such as a driver's license and pension card. Some 44,000 firms have also been issued TIN numbers.

In contrast, Ethiopia's microfinance institutions serve 3.5 million customers and require only the kebele ID for Know Your Customer (KYC) purposes. While the incidence of nonperforming loans is reported to be moderately low—around 5 percent on average—microfinance institutions report more difficulties in urban areas because it is easier for their customers to walk away from a contract and move on under another kebele identity. With customers identified by their TINs, banks are able to share credit information, but this is more difficult for MFIs without secure knowledge of their clients. Property and contract registrations are more difficult without unique, stable, and long-term identity. Those responsible for implementing Anti-Money Laundering regulations also expressed concern over the level of identity assurance provided by the current system. The need for a more robust form of identification is cited as an important element in Ethiopia's national payment systems strategy.[7]

*PSNP ID*. A few specialized types of functional ID do not require the kebele ID. One example is the client card issued to beneficiaries of the Productive Safety Nets Program or PNSP. The document issued to PNSP beneficiaries includes a photo of the head of household provided free of charge, as well as detailed information about the members of the household and the cash or in-kind amounts to which they are entitled (the latter is linked to the composition of the household). In addition to requiring more information than appears on the kebele card, another reason for not requiring it is that even though recipients may be eligible for a kebele ID, some of the poorest people might not choose to hold one or to reregister to keep their kebele ID current. Also, as explained earlier, the kebele card is not especially secure or difficult to falsify and is nowhere digitized to allow for any kind of automated verification.

---

6 Only two fingerprints are captured in registration for the TIN. This will place a constraint on how effectively enrollments can be deduplicated as numbers increase.

7 World Bank (2015). Ethiopia National Retail Payments System Strategy.

Recently however, the program has piloted G2P e-payments of the cash transfer. Preliminary reports suggest that this pilots are proceeding successfully, with reports that they offer great savings in time and convenience to recipients relative to traditional cash-based delivery. The mobile payment vehicle is Ethiopia's incipient version of M-pesa known as M-Birr. The provider is owned by the five largest MFIs as well as the Bank of Ethiopia and requires the kebele ID to establish an M-Birr account. Beneficiaries will need to apply for their kebele IDs to establish M-Birr accounts to take advantage of these systems as they are rolled out on a wider basis. Given the weaknesses of the kebele ID already described, there is a clear desire from the financial sector and mobile operators to move to a more robust form of identification.

Figure 6 shows two more functional forms of identification. In the case of the community health insurance program, there is a paper booklet issued to members that have paid a premium (and to those poor deemed eligible to have their premium paid by the government). There is no robust means of authenticating that the patient that is provided care covered by this insurance is the person that was originally enrolled. Nor is it possible to track claims and utilization electronically.

Similarly, the card issued to a public sector pensioner and the manual process of authentication by the banks, MFIs or post offices (ie., no electronic trail) could allow for significant fraud, although there appears to be little evidence of this at present. Also, in order to confirm that the pensioner is still alive, a physical visit must be performed once a year by pension fund staff.

**Figure 6: Pensioner Card and CBHI booklet**


*Source:* Authors' photos.

Functional IDs in Ethiopia are either derived from the kebele ID (passport, driver's license, voter card, TIN) or issued directly by the program in question. Only the TIN, with its deduplicated database, could help address some of the needs of the country. However, the plan is to replace the deduplication service of the revenue authority with an improved, ten finger deduplication process under the National ID Agency. This would then replace the kebele ID and would be used instead of or to generate the other functional credentials that now exist.

# 4. Looking forward—Implementing Proclamation No. 760/2012

It is rare that a country embarks upon a complete overhaul of its identification system. The 2012 Proclamation does just this, establishing the new institutional framework described in Section 2 of this report and creating two new agencies responsible respectively for rolling out new civil registration and national identification systems. It is an ambitious and potentially transformational project that will shape Ethiopia for decades to come.

## 4.1 Civil registration

The civil registration part of the initiative is more advanced than the national ID. The governance structure as described in Figure 1 is operational although there is significant variation at the regional and woreda level. Some woredas have already hired additional staff and begun training for kebele officers while others have lagged behind.

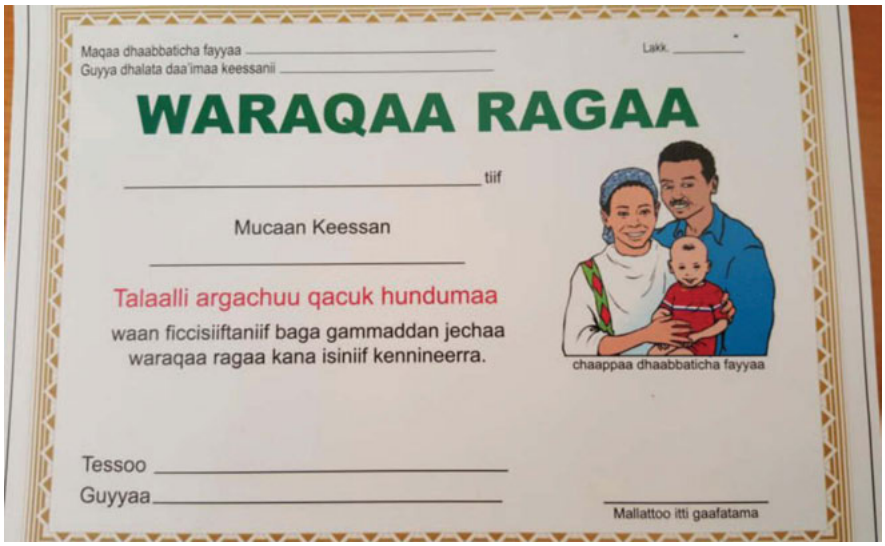
The strategy and action plan written in 2013 makes it clear that the cornerstone of the system is the kebele. Already, the kebeles perform tasks that can easily be integrated and modified to generate and issue the civil registration documents and to gather and transmit vital statistics. In many kebeles, vital statistics—births and deaths—at the individual level are gathered by health posts and kept in family folders. This reporting depends on sub-kebele groups that typically involve five family units with a lead person responsible for reporting such events. These individual, lower-level figures are then aggregated into kebele-wide figures and reported to the woreda administration on a monthly or quarterly basis. These are further aggregated up to the regional and eventually, national level. In principle then, all births and deaths are being counted on a regular basis. The population of the kebele, by age and sex, is also being tracked over time, in two-year intervals in a kind of mini-census performed by the kebele administration. This also takes into account migration.

When an individual or family leaves the kebele and does not return after six months, their health post file is declared inactive and they are removed from the population figures. When they migrate permanently, they may/should receive a letter from the original kebele which is presented to the next kebele, and a new file is created in the latter. Based on interviews however, this does not always take place.

The health posts are responsible for immunization. When a child is born, a form is filled out (in addition to adding the child to the family folder) that tracks immunizations as they take place. Upon completion of immunizations, typically after nine months, a certificate such as the one shown in Figure 7, is filled out, stamped with the specific stamp of the kebele, and signed by the health worker. IT contains the mother's name, date of birth, and a number assigned to the newborn consisting of the sub-kebele and house numbers and the child's own number (in sequential order of birth). According to interviews, this is an important document in that it is required for school registration and other matters requiring proof of the child's age. Presumably, it also serves the function of ensuring that children attending school have been fully vaccinated.[8]

8 It is not clear how long this practice has been in place, and at least one kebele visited did not report issuing such certificates.

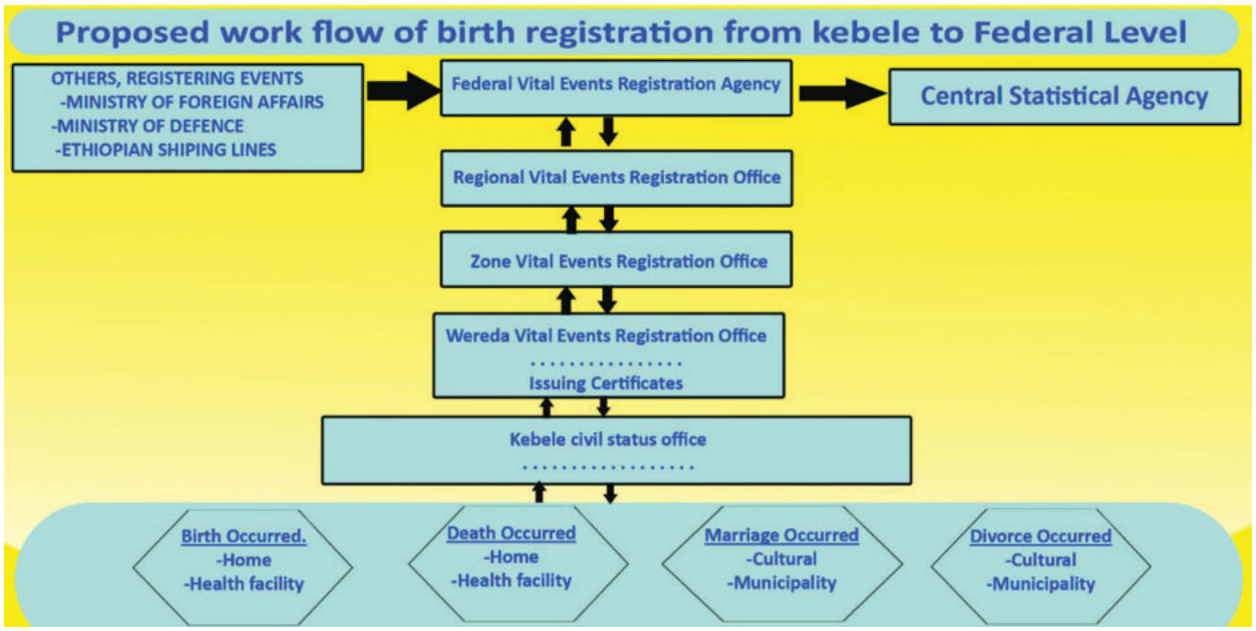
**Figure 7: Immunization Certificate**




*Source:* Authors' photo.

To the extent that there are staff already performing these operations at the kebele level, it would seem straightforward to convert the existing processes into those required for civil registration. Figure 8 shows the process envisioned for the flow of data. Compared to the present situation, the difference is that only aggregated figures on these vital events are transferred upwards along the institutional chain. The major changes that must be incorporated for the purposes of birth registration are (i) the transfer of *individual level* records to the RVERA and ultimately, VERA recordkeeping systems and (ii) adding the issuance of standardized certificates. This would require a shift from the manual, paper-based books maintained at

**Figure 8: The Envisioned Flow of Civil Registration Data from the Kebele**




*Source:* Towards sustainable vital events registration and vital statistics system of Ethiopia: Strategy and Action Plan, July 2013–2018.

the kebele office, to a record that would be transported or sent online to the woreda level database. The process of issuing certificates would require an additional step to move the physical document produced centrally down to the kebele (the exact design of the certificates and their security features was being discussed at the time of writing).

The VERA has recognized that there is significant variation in the capacity and physical infrastructure of the kebeles and initially at least, many will not have the conditions in terms of staff and space (much less computers and connectivity) to implement the new system. This has led to a plan with three phases wherein the 3,000 or so most prepared kebeles implement the system first. If all kebeles were eventually operating as civil registration offices, it would result in one of the most extensive such networks in Africa and be one of the most accessible in the world. While this is a major advantage of the kebele infrastructure, the efficiency of the system depends on how well this network of kebele offices is able to transfer data through the WOREDA-net system. It is also essential that it can operate off-line when necessary.

One element in the process that is not elaborated in the action plan is the issuance of unique ID numbers on the birth certificates that VERA issues. The integration of the civil registration system and in particular, the birth and death registration processes and data are crucial elements in building the new identification system. This is discussed in Section 5.

## 4.2 National ID

The original concept and justification document for a national ID to replace the kebele ID system was drafted in 2009. A steering committee led by the Ministry of Information Communication Technology (ICT) and the security agency, INSA, was constituted and hired a technical cell to develop the procurement documents. The request for proposals was issued through the World Bank's procurement website. The tender eventually issued covered the purchase of an Automated Fingerprint Identification System (AFIS), enrollment kits, the actual enrollment process, and the issuance of both smart cards and regular, polycarbonate cards. The enrollment was to cover residents aged 18 and above and 10 fingerprints would be captured.

As in the case of the civil registration, the rollout of the plan was phased. In the first year, the equipment and infrastructure would be installed, including the AFIS. In the next two years, enrollment of approximately 6 million people in a 150 km radius around Addis would be enrolled. The rest of the country would be enrolled in years 4 and 5.

Unlike VERA, the 'organ' that would administer the national ID card and implement that part of the proclamation has not been constituted. Although both were scheduled to begin operation on July 1, 2016, VERA actually began in August of 2017, and the NID agency has still not begun implementation. The gap between the implementation of the two projects could have implications. The principle of linking the civil registration processes and database to that of the national ID system has been well accepted since the beginning of the project. A representative from the latter meets regularly with the VERA Council. The stated intention is to include a centrally issued and unique national ID number on each birth certificate issued. An important issue facing VERA is how to ensure that the number that would be issued at birth would ensure uniqueness and, related to this, that only one birth certificate would be issued to one individual.

By assigning the NID number at birth and including it in the birth certificate to provide a consistent lifetime identifier, every Ethiopian and/or resident of Ethiopia can have a unique lifetime number. If the NIDs of the parents are included as part of the birth documentation, this also strengthens the intergenerational links in the ID system. If the parents' numbers are deduplicated biometrically, the potential for multiple birth certificates being issued would be reduced. In any case, at the point that the child reached a certain age, his biometrics would be captured again and any duplicates that had entered the birth registration system would be corrected (see below). The options for integrating the NID number and the civil registration processes, among other things, are discussed in the next section.

# 5. Options going forward

Ethiopia's identification system is at a crossroads. A two-pronged effort is under way to create a completely new system to register births, deaths, and other vital events along with the biometric enrollment of the entire adult population and issuance of the country's first secure form of identification with a national scope. This section explores some key policy and implementation issues that must be addressed in order to ensure that these efforts yield the potential benefits of a good identification system. These include but are not limited to:

**a.** Digitizing the civil registration system
**b.** Linking the unique national ID number to the birth and death certification process
**c.** Determining the structure of the unique ID number
**d.** Ensuring the integrity of the civil registration and national ID databases
**e.** Protecting personal data and minimizing potential for its misuse
**f.** Managing the transition from the kebele ID to the new identification system
**g.** Implementing a sustainable financing model

## 5.1 Digitizing the civil registration system

VERA's intention has always been to introduce the new civil registration system using electronic records and digital processes. Rather than further delay the launch, VERA decided to go ahead in August 2016 despite the fact that only manual, paper-based processes could be used. As a result, Ethiopia will face the same challenge as many other countries in shifting from paper to digital records and processes.

Based on preliminary research by the World Bank's ID4D program, it would appear that there are no off-the-shelf products that could be considered. Plan International, with support from the African Development Bank, is developing an open source software platform called OpenCRVS which may be a viable option at some point in the future. Most of the experiences of moving from paper to digital have entailed customized solutions where a firm with experience in work flow and information management has been contracted to build a system that allows for manual processes to become automated. Recent examples include São Tomé and Principe and Lesotho.

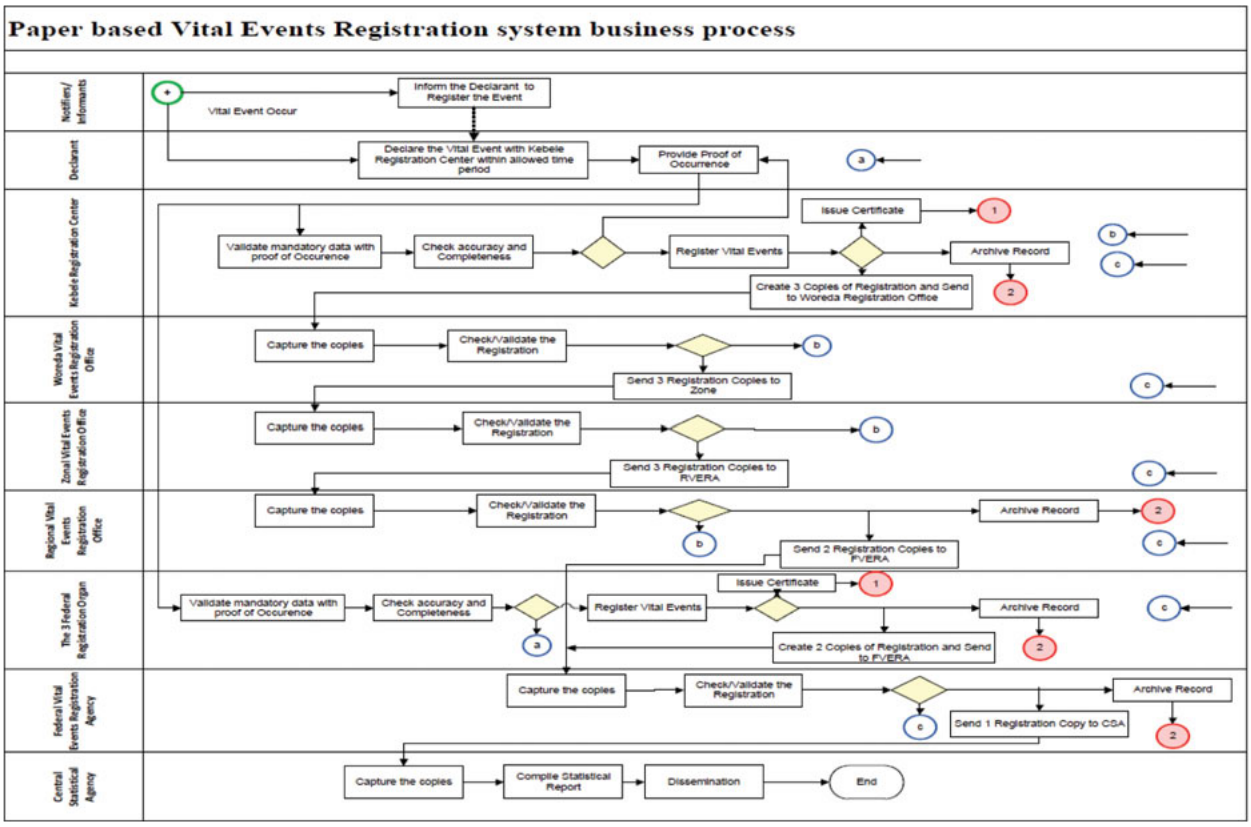
The first step in such a transition is to clearly document existing paper-based processes. Figure 9, produced by VERA, describes the complex web of transactions and records that currently flow in paper form, starting at the kebele all the way up to the central statistical agency and federal layer of VERA.

## 5.2 Linking the unique national ID number to the birth and death certification process

The registration process that was launched in August 2016 uses manual processes and issues a number for each person which contains logic. As the national ID does not yet exist, there is no link with it at this point. In the long run however, the VERA intends to move to a digital process and to link with the national ID toward the eventual creation of a seamless system and a complete population register.

In order for national ID numbers to be included in the birth certificate and the corresponding civil registry database, the National ID Agency will have to provide these numbers to VERA. There are several ways that

**Figure 9: Process Flow for Current Paper-Based System in Ethiopia**




*Source:* VERA (2017).

this could be done, and each depends on the business process flow that begins at the kebele office. One possibility would be for the kebele to make an online request for a unique ID number each time a birth certificate was being issued. In this case, the kebele official would have to provide biographic information in electronic form and, once submitted, could receive a unique ID number. This number could be provided to the parents with the understanding that the birth certificate would be generated centrally and they could pick it up in a few weeks. The certificate would include the unique ID number and it would also be included in the CR and NID databases. Alternatively, if birth certificates were printed and distributed by the kebele, this could be done immediately, or within a relatively short time.

The online approach may work in some kebeles, particularly in urban areas and may eventually be appropriate throughout the country. In the short run however, connectivity issues would preclude this approach in most kebele offices. Alternative, off-line processes will be the norm at least in the early years of the system. There are several options and variants for off-line generation of the unique ID number and inclusion of this number in the birth certificate.

## 5.3 Determining the structure of the unique number

A key decision is the structure of the unique national ID number. The number in most countries is constructed using some information specific to the individual.[9] This could include attributes such as gender, name, or place of birth but by far the most common personal data used is the date of birth (DOB). Using information

9 See: https://en.wikipedia.org/wiki/National_identification_number

about the individual allows for some simple checks; a number that indicated a male aged 75 could not be used by a young woman, for example. Most of these numbers were created before there were ways to include secure photographs in credentials or, more recently, to include machine-readable information that largely obviates the need to look for identifying information in the number itself. The most sophisticated variant of authentication is biometric and is being used in national IDs through smart cards in some countries.

While technology is making the case for having logic in the ID number less compelling, increasing concerns about privacy are emphasizing the negative aspects of having personal information contained in the number. A small but growing number of countries has rejected 'intelligent' numbers in favor of random or so called 'dumb' numbers that do not in any way provide information about the individuals to whom they correspond. These include the Netherlands, Nigeria, Turkey, and Uruguay.[10] The most well documented case is India's Aadhar number.[11] Box 1 compares number structures in India, Indonesia and South Africa.

The need to assign numbers to both a stock of existing people (mass registration) and a flow of newly born people have some implications for the process and possibly also for the numbering system. In cases like South Africa and Indonesia, the inclusion of date of birth (as well as location in the case of Indonesia)

### Box 1: Unique numbering systems globally

Countries have developed a wide range of NID numbering systems. Some use "dumb" numbers that reveal nothing about their holders. India's random Aadhaar is an example. Many use "intelligent" numbers that can include digits representing: location of registration, date of birth, and gender, as well as an individual PIN. Examples include South Africa's ID number and that of Indonesia. "Intelligent" numbers can also include digits or letters derived from the name of the holder (Mexico) or derived from the phonetic sound of the name of the holder (the Soundex-based numbers used for the driving licenses in many US states). There is no uniformity.

By their nature, "dumb" numbers can be shorter for a given population than "intelligent" numbers because they can use all possible combinations of digits. It is also argued that they protect the privacy of their holders better, and that they are less prone to include characteristics, such as gender, that can change over the lifetime of an individual. In some numbering systems, it is quite possible to derive the number from knowledge of the name and birthday of the holder, and this could open the door to identity theft. On the other hand, especially if connectivity is limited, it could be argued that the information in a number can be useful in helping to authenticate the holder against a credential, at least approximately (male, 55 years old). Photos and fingerprints, as appear on many ID cards today are, of course, better identifiers, and especially with improving connectivity, there is probably some sentiment in favor of dumb or random numbers.

Many ID numbers include a check digit to help prevent transcription errors. This is good practice. Check digits can be generated through many different algorithms. The most sophisticated such as the Verhoeff algorithm will be able to detect all of the most common errors—single-digit errors and transpositions of two adjacent digits—but are complex to calculate. Some systems, such as South Africa's, use the Luhn algorithm which is simpler and can detect almost all, but not all, such common errors.

10 New Zealand's National Health Index number, although not a national ID, is issued at birth, and is also a random number.
11 Aadhar is not a national ID as it applies equally to all residents of India and does not constitute evidence of citizenship or legal identity.

Thus, for example:

**India's** Aadhaar is a 12-digit number XXXXXXXXXXXC with the first 11 digits random and the 12th a check digit derived using Verhoeff's algorithm.

The **South African** 13-digit ID number is of form YYMMDDGXXXNRC. Where YYMMDD represents date of birth, GXXX is a gender marker plus 3-digit PIN (5000+ is male, 4999-female), and N is nationality: 0 for South Africa and 1 if not, R is a racial identifier, now redundant C is a check digit, generated by the Luhn Algorithm.

**Indonesia's** 16-digit KTP number is of the form PPRRSSDDMMYYXXXX where PP is a 2-digit province code, RR is a 2-digit regency or city code, SS is a 2-digit subdistrict code, DDMMYY is date of birth, and XXXX is a 4-digit personal number.

makes it possible to cover the population with only a relatively short personal number. South Africa has roughly 1.5 million births per year or around 4,000 per day. This flow can easily be accommodated with the 4 digit GXXX. However, if ID cards were to be issued to a large stock of mature individuals who were not sure of their dates of birth, it is quite possible that reported birth dates could cluster as people report their ages approximately. In that case, the numbering system could be inadequate. One question for Ethiopia is therefore whether the accuracy of birth knowledge is sufficient to ensure a smooth flow of numbers issued at birth or, indeed, to simply use the birth number as the ID number. If the answer is 'no', this would be more complicated.

Another important consideration is whether NIDs will be issued centrally or in a decentralized environment. Typically, NIDs are administered centrally, increasingly based on a biometric enrollment, a secure digital credential and with a single agency responsible for issuing unique number. This makes it possible to use a numbering system that is independent of the location of registration—the random-numbered Aadhaar is an example.

With different languages and alphabets, Ethiopia's NID number should be strictly numeric with no alphabetic characters. With a population of about 100 million, a dumb numbering system would need to have at least 9 digits, or 10 including a check digit. To increase sparseness this could be increased to 11, which would then be scaled similarly to the Aadhaar system relative to the population. "Intelligent" numbers would be considerably longer. For example, if the number were to denote each of the 16,000 kebeles this would take up at least the first 5 digits (this would resemble the number in Indonesia).

## 5.4 Ensuring the integrity of the civil registration and national ID databases

The process described above addresses the flow, but there remains the challenge of dealing with the stock of the population. NID numbers will need to be assigned to three cohorts of Ethiopians:

- Infants: the youngest cohort (say 1–5) who will come online as the flow of birth registration increases.
- Adults: the stock of citizens over 18 who are now identified by kebele IDs. Few of these will have been registered at birth or have birth certificates.
- Juveniles: the stock of those less than 18 but over the age of 5. These will not yet have kebele IDs and few will have birth certificates. Possibly they will be registered in blocks at schools.

One possibility is to consider using random or block random numbers. Under this arrangement, Ethiopia adopts a 10-digit number, 9 + a check digit. This is sufficient to cover up to 999,999,999 people, allowing considerable flexibility. These numbers are divided into blocks. One block is assigned to the NID system. This assigns the individual numbers to those registered through the centralized NID process. The other block is assigned to the CRVS system. This can either assign numbers centrally (if connectivity is adequate) or can assign sub-blocks of numbers to each registration unit to enable it to provide the numbers immediately in a decentralized way. The biographic and biometric data collected by the two processes will in each case be linked to the number; this will remain constant through the lifetime of the individual.

One complication is that only the numbers issued by the NID system will have undergone a rigorous process of deduplication. A variant of this approach could therefore be to adopt an 11-digit number, with the first digit denoting the registering entity:

0 for a number issued by the CRVS system, normally at birth

1 for a number issued by the NID system. This would signify a number that has been through the biometric and biographic deduplication processes of the NID. At that point the old ID and number would be cancelled.

The basic ID number (digits 2 through 10) would remain the same.

The check digit would change to reflect the change in the initial digit.

Such an arrangement would preserve the continuity of identity over the life cycle but at the same time distinguish between those who had achieved the age of national registration and those who had not. This could be important, for example, in ensuring that individuals seeking to open bank accounts or to vote had identities that had been fully deduplicated.

## 5.5 Protecting personal data and minimizing potential for its misuse

In 2017, the "Principles on Identification for Sustainable Development" were endorsed by a wide range of international organizations including development agencies, major foundations, and private sector associations that support or help implement national identification systems. One of the ten principles (see Annex 1) is aimed at ensuring that personal data and privacy are protected. Specifically:

> *"Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework."*

In Ethiopia currently, issues related to privacy and data are handled by the Ministry of Communication. However, there is no legislation in place that meets international standards in this area. The Annex provides a generic model law on personal data protection. It is important that such legislation and the human resources to apply it are developed before or at least in parallel with the creation of a new, digital identification system.

## 5.6 Managing the transition from the kebele ID to the new identification system

As noted, most adults appear to have and regularly use their kebele IDs to perform many identification-related tasks in their daily life. It will take some time to enroll the population and replace this ID with the new, digital one. In the interim, transition arrangements will have to be put into place. In some cases,

there may be good reason to re-authenticate with the new digital ID. For example, mobile connections registered with the kebele ID could be registered again but this time with the more robust ID. This would be particularly important for mobile money and for the microfinance sector as it would be the first time that a truly unique identifier with the capacity of biometric authentication would have been available.

## 5.7 Implementing a sustainable financing model

The World Bank plans to provide financing through the Global Financing Facility (GFF) to help VERA improve its systems and its capacity. However, the available funding is not enough to achieve the shift from a manual, paper-based system to an automated, digital system. While there is no concrete estimate available, it would likely entail a major infrastructural investment and would take several years to implement. In the meantime, VERA officials report that the massive influx and movement of paper files is already creating problems and delays. The faster that the current system can be digitized, the better the chances of stabilizing the system and maintaining a database that is up to date and accurate.

The national ID law still appears to be far from being implemented. The original planning took place almost a decade ago, and there have been many developments and relevant international experiences that suggest that it may be worth reconsidering certain elements of the plan, including the type of technology that may be most efficient. This could lead to a reassessment of the cost of the new system. Recent experiences suggest that these costs can be reduced if certain choices are made regarding the nature of the database being created as well as the type of credential (card) that is chosen.

At the same time, there is a growing understanding of the potential fiscal benefits of modern identity schemes. In particular, the use of digital identification for better authentication has been shown to reduce 'leakages' and save the government millions. It can also enable better and cheaper authentication for which the private sector—particularly the telecom and financial industries—are willing to pay.

# 6. Summary and conclusions

The passage of legislation establishing a new identification system in 2012 was an important milestone and confirmed that this is a government priority. However, implementation progress has been slow and, in some ways, suboptimal. The launch of VERA's vital events registration across the country, while a major advance for CRVS, was done without the benefit of a digital infrastructure that would have leapfrogged the manual, paper-based process that has been so difficult to move away from in so many developing countries. The intention to remedy the situation is clear, but the current financing that is available does not appear to be sufficient.

The national ID remains a concept five years after the proclamation was issued to create it. If anything, this will require more resources than the modernization of the CRVS, at least in the short run. Meanwhile, the cost of continuing to rely on the kebele ID in the context of urban migration, the rise of mobile money and the digital economy, and the expansion of coverage of social programs and spending will steadily increase. International experience suggests that planning, procuring, and rolling out a new national ID will take a minimum of 3–5 years. Ideally, the shift to a digital CRVS and the introduction of a national e-ID would be implemented in parallel, and the respective systems would be interoperable from the start.

# References

Gelb, Alan, and Julia Clark. (2013a). "Identification for Development: The Biometrics Revolution." CGD Working Paper 315. Washington, DC: Center for Global Development.

World Bank (2015). "Ethiopia National Retail Payments System Strategy."

Zewoldi, Y. (2013). "Towards sustainable vital events registration and vital statistics system of Ethiopia: Strategy and Action Plan, July 2013–2018," UNFPA.

# **Annex:** Generic privacy and data protection legislation

### Privacy and Data Protection Law

| Chapters | Articles | Suggested Content |
|---|---|---|
| **General Provisions** | Subject matter | This article shall indicate the subject matter of the law, which is to establish the provisions relating to the processing of personal data with a view to protecting the fundamental rights and freedoms of individuals |
| | Scope | This article shall indicate the scope of application of the law with relation to its object, subjects and territory:<br>**Object:**<br>The law shall apply to the processing of personal data wholly or partly by automatic means, as well as to the processing of personal data by nonautomated means when the personal data forms part of a filing system or are intended to form part of a filing system<br>**Subjects:**<br>The law shall apply to the processing of personal data performed by any person or entity<br>**Territory:**<br>The law shall apply to the processing of personal data performed:<br>▪ Within the scope of activities of an establishment of the data controller situated in the territory<br>▪ Outside the territory, in a location where national law is applicable under international law |
| | Exclusions | This article shall indicate the cases where the law does not apply. It is suggested that the law does not apply to the processing of personal data by an individual exclusively within personal or household activities |
| | Definitions | This article shall provide definitions for all the main terms used throughout the law, including especially on:<br>▪ Advertising/direct marketing<br>▪ Consent by the data subject<br>▪ Data controller<br>▪ Data processor<br>▪ Filing system/file<br>▪ Interconnection<br>▪ Personal data<br>▪ Processing<br>▪ Recipient |

| Chapters | Articles | Suggested Content |
|---|---|---|
| | | ▪ Sensitive data<br>▪ Third party (in the context of personal data processing) |
| **Processing of Personal Data** Section I General principles | Principles relating to the processing of personal data | This article shall indicate the principles that shall be complied with in the processing of personal data:<br>▪ The principle of lawfulness<br>▪ The principle of transparency<br>▪ The principle of proportionality<br>▪ The purpose limitation principle<br>▪ The principle of accuracy<br>▪ The principle of the data retention length |
| Section II Requirements for the processing of personal data | General requirements | This article shall indicate the general requirements that apply to the processing of personal data. It is suggested that these requirements be the following:<br>▪ The unambiguous and express consent of the data subject (which may or may not oblige written form) or<br>▪ The processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract or<br>▪ The processing is necessary for compliance with a legal obligation to which the controller is subject or<br>▪ The processing is necessary in order to protect the vital interests of the data subject if the data subject is incapable, physically or legally, from giving his consent or<br>▪ The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed or<br>▪ The processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the data subject |
| | Specific requirements for sensitive data | This article shall indicate the requirements that apply to the processing of sensitive personal data, which shall be the unambiguous, express, and written consent of the data subject<br>▪ The processing is carried out (i) in the course of legitimate activities by a foundation, association or any other nonprofit-seeking body with a political, philosophical, religious, or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects and (ii) with the unambiguous and express consent of the data subject or |

*(continued)*

| Chapters | Articles | Suggested Content |
|---|---|---|
| | | ▪ The processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent or<br>▪ The processing relates to data which are manifestly made public by the data subject, provided that consent to their processing can be legitimately inferred from his statements or<br>▪ The processing is necessary for the establishment, exercise, or defense of legal claims and is done exclusively with that purpose or<br>▪ The processing is, for reasons of public interest, necessary for the performance of legal or statutory obligations of the controller, including for the performance of investigation activities by competent authorities or<br>▪ The processing is permitted by a legal provision |
| | Specific requirements for data relating to health and sexual life | The processing of data relating to health and sexual life shall only be done under the following circumstances:<br>▪ The unambiguous, express, and written consent of the data subject or<br>▪ As required or permitted by law or<br>▪ The processing is necessary for purposes of preventive medicine, medical diagnosis, consented medical care or treatment, management and statistics of health services, or when there is a medical emergency<br>The processing can only be done by a health professional duly authorized as such or by another person subject to professional secrecy |
| | Specific requirements for data relating to illegal activities | This article shall establish the conditions for the processing of data relating to subjects suspect of illegal activities, crimes, and misdemeanors, as well as to subjects to whom penalties, security measures, fines, and ancillary sanctions are applied. Such processing shall only be performed by a public competent entity provided that (i) there is a legal provision allowing such processing or (ii) if necessary for the performance of the legitimate purposes of the controller, except where such purposes are overridden by the fundamental rights and freedoms of the data subject |
| Section III Communication | Communication of data to a controller or to a third party | This article shall establish the requirements for communicating data to a recipient that will process the data for its own purposes (in which case the recipient is also a controller for its specific autonomous purpose) or to a recipient that will process the data neither for its own purposes nor for the purposes of a controller (in which case it shall be a third party)<br>In this case, communication shall be subject to:<br>▪ The unambiguous and express consent of the recipient unless<br>  ▪ The communication results from law or judicial decision or<br>  ▪ The data has been collected from publicly accessible sources in compliance with their conditions of consultation and use or<br>  ▪ The communication is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract or |

| Chapters | Articles | Suggested Content |
|---|---|---|
| | | ▪ The communication is necessary for compliance with a legal obligation to which the controller or the recipient are subject to or<br>▪ The conditions that permit the processing of personal data without the data subject's consent are met<br>The communication of data among authorities tasked with investigation, prevention, and repression of crimes shall be able to be done without consent of the data subject |
| | Communication of data to a subcontractor | Communication of data to a subcontractor shall be subject to a contract or other legal document between the controller and the subcontractor under which the subcontractor undertakes to comply with this law and act in accordance with the controller's instructions<br>The subcontractor shall further be subject to the following obligations:<br>▪ Not communicate the data to other recipients<br>▪ Comply with the security measures established in law<br>▪ Destroy or return the data upon the ending of its relationship with the controller<br>▪ Make available to the data controller the data that are being processed and information regarding the way the data are being processed |
| Section IV Rights of the data subjects | Right to information | This article shall indicate the information that the controller shall make available to the data subjects. It is suggested that this information includes:<br>▪ The identity and point of contact of the controller<br>▪ The purposes of the processing<br>▪ The compulsory or optional nature of the responses, as well as the consequences for nonresponses<br>The existence of the right of access to and the right to rectify or eliminate his/her data<br>The information shall be provided at the time of the collection of the data (if the collection is made directly from the data subject) or within a reasonable period of time after their collection (if the collection is not made directly from the data subject)<br>Such information does not have to be provided:<br>▪ If so provided in law<br>▪ For reasons associated with state security or criminal prevention/ investigation/repression<br>▪ If the provision of the information is impossible or demands disproportionate efforts, such as in the case of data processing for statistical, historical, or scientific investigation purposes<br>▪ When the processing is carried out solely for journalistic purposes or for the purpose of artistic or literary expression |

*(continued)*

| Chapters | Articles | Suggested Content |
|---|---|---|
| | | In case the collection of data is done in open networks, the information is considered given by means of privacy policies that include:<br>▪ The information above provided<br>▪ The information that the data can circulate in the network without security conditions and hence there is the risk they may be seen and used by non-authorized third parties |
| | Right of access | This article shall indicate that the data subject shall have the right to obtain from the controller, without restrictions, delays, or excessive costs, information on:<br>▪ Whether the controller is processing data of the subject<br>▪ The specific data being processed and any available information on the origin of such data<br>▪ The purposes of the processing<br>▪ The categories of data being processed<br>▪ The recipients or categories of recipients to whom data is communicated<br>The right of access may be refused when access may negatively impact state security, criminal prevention/investigation/repression, judicial secret, freedom of information and of the press, or impact unreasonably upon the privacy of other individuals |
| | Right to object | This article shall indicate that the data subject shall have the right to object to the processing of his data. The data controller shall cease the processing upon such request unless:<br>▪ The law provides otherwise<br>▪ Opposition may negatively impact state security, criminal prevention/investigation/repression, judicial secret, freedom of information and of the press<br>▪ The processing of data does not require the data subject's consent |
| | Right of rectification, update, and deletion | This article shall indicate that the data subject shall have the right to request his data to be rectified, updated, or deleted if their processing does not comply with the law<br>The data controller shall proceed with the rectification, update, or deletion in due time and notify any recipient to undertake such actions as well<br>The data controller shall, however, block and/or retain the data in the following cases:<br>▪ Legal provision or order by competent authority<br>▪ If the blocking and/or retention is necessary for prosecuting a legitimate interest of the controller<br>▪ If the data are being used for purposes of a criminal investigation<br>▪ If the data relate to credit and solvency when the data subject does not have his credit situation regularized |

| Chapters | Articles | Suggested Content |
|---|---|---|
| | Automated individual decisions | This article shall indicate that a person shall not be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.<br><br>However, a person may be subject to a decision of this type if such decision:<br><br>▪ Is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view or<br><br>▪ Is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests |
| Section V Security measures | Security measures | This article shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing<br><br>Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected |
| | Special security measures | This article shall require from the data controller the implementation of specific security measures in case the data being processed are sensitive data; data relating to health and sexual life; data relating to illegal activities, crimes, or misdemeanors; data relating to credit and solvency; and data relating with video surveillance<br><br>In this case, the controller shall adopt the measures required to:<br><br>▪ Prevent access to the files and premises used for processing by non-authorized persons<br><br>▪ Prevent that the data can be read, copied, altered, or removed by non-authorized persons<br><br>▪ Prevent the non-authorized introduction, learning of, alteration, or deletion of data<br><br>▪ Prevent that the systems of automated data processing be used by non-authorized persons<br><br>▪ Guarantee that only authorized persons can have access to the data covered by their respective authorization<br><br>The data relating to health and sexual life shall be logically separated from the remainder data |

*(continued)*

| Chapters | Articles | Suggested Content |
|---|---|---|
| Section VI International transfer of personal data | Transfer of data to third countries | The transfer of data outside the territory shall be subject to the following:<br>▪ The data subject gives his unambiguous, express, and written consent or<br>▪ The recipient warrants, contractually, before the controller, that it is subject to a law or binding system that is substantially similar to the protection provided for in local law or<br>▪ The recipient warrants, contractually, before the controller, that it will comply with obligations similar to the ones foreseen in local law or<br>▪ The transfer is made under international treaties or<br>▪ The transfer is made to a country that the government or supervisory entity have considered that has a level of protection of personal data similar to the one afforded in the territory<br>▪ In the case of companies belonging to the same group, international transfers among them can be made provided they adopt internal common provisions relating to data protection that comply with the requirements of local law<br>It may also be evaluated to permit the international transfer of data in the following cases:<br>▪ The transfer is exclusively aimed at responding or making a request for humanitarian assistance or<br>▪ The transfer is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract or<br>▪ The transfer is necessary or legally required for protecting a public interest or for exercising or defending a right in a judicial procedure or<br>▪ The transfer is necessary in order to protect the vital interests of the data subject or<br>▪ The transfer is made from a publicly accessible source |
| **Supervisory Framework** | Supervisory entity | This article shall indicate the supervisory authority for data protection issues<br>In the short term, it is suggested that either the Ministry of Justice or the Ministry of Communications are appropriate choices, with the support of a specific team focused on data protection and privacy matters<br>In the medium and long term, it is suggested that a supervisory data protection entity is created. This article can already indicate that a law may create a specific data protection authority |
| | Powers of the supervisory entity | This article shall indicate the powers of the supervisory entity, which shall include supervising compliance with the law, issuing orders to the controllers in accordance with the law, receiving complaints and opening and pursuing misdemeanor procedures, and applying the respective fines |

| Chapters | Articles | Suggested Content |
|---|---|---|
| | | In the medium and long term, upon the creation of a specific data protection authority, it is suggested that, in addition to the powers that would currently be exercised by one of the ministries above indicated, the authority would have the power to receive notifications and/or issue authorizations for data processing. In such a situation, then, the Privacy and Data Protection Law should be amended to establish the situations and conditions for notification and/or authorization<br><br>All public and private entities shall cooperate with the supervisory authority, by means of providing the requested information and allowing access to their systems and documentation relating to the processing of personal data |
| **Sanctions Framework** | Misdemeanors | This article shall establish the fines applicable to the breach of the law<br><br>Different amounts of fines shall be provided in light of the type of breach and its seriousness<br><br>Application of fines shall not prevent the controller from complying with the law, whenever possible |
| | Determination of the amount of the fine | This article shall indicate that certain criteria shall be taken into consideration when determining the amount of the fine, such as the unlawfulness of the act, the negligence of the agent, and the benefits obtained with the misdemeanor, as well as the economic situation of the agent |
| | Destination of the fines | This article shall indicate to whom the amounts of the fines are destined (e.g., 50% for the State and 50% for the entity that applies them) |
| | Crimes | This article shall establish that breach of certain provisions of the law is a criminal offense. It is suggested that the following be criminal offenses: process data in breach of the purpose limitation principle; perform an illegal interconnection; unauthorized access to personal data; unauthorized destruction or damage to personal data; disobedience in complying with legitimate orders relating to the processing of personal data; and breach of the obligation of secrecy |
| | Ancillary sanctions | This article shall provide the possibility of applying ancillary sanctions, which may include the loss of assets used to commit the breach and the interdiction of continuing to perform the processing |
| | Crime and misdemeanor met | This article shall indicate that if the conduct is simultaneously a crime and a misdemeanor, it shall be punished as a crime |
| **Final Provisions** | Coordination with legal other provisions | This article shall indicate that this law does not prejudice the application of the provisions indicated in other laws for data processing, including when the requirements therein indicated are more demanding than the ones herein provided |
| | Subsidiary application | This article shall indicate that the sanctions framework provided in the Privacy and Data Protection Law do not preclude the application of sanctions indicated in special law, nor the resort to administrative or judicial means to guarantee compliance with the provisions of the law |

*(continued)*

| Chapters | Articles | Suggested Content |
|---|---|---|
| | Sectorial regulation | This article shall indicate that additional regulation on specific sectors or to address specific matters may be approved |
| | Entry into force | This article shall indicate when the law enters into force<br>A reasonable period of time shall be indicated so as to allow current data processing to become in compliance with the law |

worldbank.org/id4d

ID4D
IDENTIFICATION FOR DEVELOPMENT

WORLD BANK GROUP