

DATA PROTECTION CODE OF PRACTICE **FOR** DIGITAL IDENTITY SCHEMES IN AFRICA

Africa
Digital
Rights
Hub



DATA PROTECTION CODE OF PRACTICE FOR DIGITAL IDENTITY SCHEMES IN AFRICA

Africa
Digital
Rights
Hub



Copyright © 2019 by Africa Digital Rights Hub

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form by any means electronic, mechanical, recording, photocopying or otherwise without the prior written permission of the author.

This book may not be lent, sold or hired out or otherwise by way of trade or whichever way in any form or language or binding or cover without the prior written permission of the author.

ISBN: 978 - 9988 - 54 - 744 - 8

For more information, copies, comments and suggestions contact: ADRH on + 233 (0) 302 909 482

Designed & Printed by G-Pak limited

+ 233 (0) 205 000 565

CONTENT

1.	ACKNOWLEDGEMENTS	vii
2.	DATA PROTECTION/PRIVACY IN AFRICA	1
3.	DIGITAL IDENTITY FOREWORD	4
4.	ISSUES ON THE AFRICAN CONTINENT	7
	Legislative Landscape	7
	Identity Crisis	7
	<i>Taking Part in the “Fourth Industrial Revolution”</i>	8
	<i>Nobody Wants to be Left Behind</i>	8
	<i>Not all are Starting from the Same Position</i>	9
	<i>Privacy Legislation at Present in Africa</i>	9
	<i>Identity Schemes at Present</i>	9
5.	ID SCHEMES	11
	Stakeholders	11
	<i>Individuals</i>	11
	<i>Governments</i>	11
	<i>Private sector</i>	12
	<i>International Organisations and NGOS</i>	12
	<i>Development Partners</i>	12
	ID Scheme Lifecycle Considerations	12

6. ARGUMENTS SURROUNDING ID SCHEMES 15

Types of Identity Scheme Providers 15

Types of Identity Schemes 15

Dangers Surrounding Digital ID Schemes 15

Unfairness 15

Expensive 16

Intrusive and unsafe 16

Inclusion vrs. Exclusion 16

7. ORGANISATIONAL ACCOUNTABILITY 17

Privacy Management 17

Privacy Expertise 18

Privacy By Design 19

Privacy By Default 20

Privacy Impact Assessment 20

Records of Processing 21

Supervisory Authorities and Consultation 24

Breach Notification 26

Third Party Management 26

Codes of Conduct and Certification 26

Measuring, Monitoring, Audit and Improvement 27

8. PRIVACY PRINCIPLES 28

Legitimate Legal Basis 29

Special Category Data 29

<i>Mandatory vs Optional Schemes</i>	30
Purpose Limitation	33
<i>Primary Purposes of Use</i>	33
<i>Secondary Purpose of Use</i>	33
<i>New Purposes</i>	33
<i>Third Party Usage/Connections</i>	34
Collection Limitation	35
<i>Anonymisation</i>	35
<i>Pseudo – Anonymisation</i>	36
<i>Through life Minimisation</i>	36
<i>Systems Design</i>	36
<i>DNA/Biometric data</i>	36
Fair Processing, Privacy Notices and Transparency	38
<i>Notices</i>	38
<i>Updating of Notices</i>	40
Data Quality	40
<i>Design</i>	40
<i>Verification</i>	40
<i>Changes</i>	41
Storage Limitation, Retention and Deletion	41
Individual Rights	42
<i>Access</i>	43
<i>Erase</i>	43
<i>Rectification</i>	44

<i>Objection</i>	44
<i>Restriction</i>	44
<i>Portability</i>	44
<i>Automated Decision Making</i>	45
<i>Lodge Complaint/Remedy</i>	45
<i>Regulatory Rights</i>	45
International Transfers of Data	46
 Security	 47
<i>Risk Assessment</i>	48
<i>Controls</i>	48
<i>Breach Notifications</i>	49
<i>Managing Third Parties</i>	50
<i>Data Access</i>	52
 9. ADDITIONAL ISSUES FOR CONSIDERATION	 53
Marriage Name Changes Forward and Back	53
Metadata Tagging	53
Cultural Norms	53
Digital Resilience	54
Search Functionality	54
Name Spellings, Spoken Language and Identity	55
Index of Words	56
Appendix – Research List	59
Appendix A – Identity Assurance Principles	61
Appendix B – Privacy Laws Across Africa	75

ACKNOWLEDGEMENTS

On 20th November 2018, during the maiden Data Protection Africa Summit in Balaclava, Mauritius, the multi-stakeholder Focus Group (made up of data protection authorities, identity system stakeholders, industry players, and donor agencies) looking at *'Data Protection and the National Digital Transformation Agenda; The Case of Personal Identity and Addressing'* recommended among other things the need for a data protection code of practice for digital identity schemes in Africa.

The Focus Group recognised the growing importance of digital identification for Africa's digital economy and taking cognizance of the risks associated with such systems, stressed on the need to ensure adequate data protection and privacy safeguards. The Focus Group however noted that the challenges barring effective implementation of data protection/privacy standards within identity systems were due to - among other things - the lack of capacity, knowledge and expertise. The Africa Digital Rights' Hub (ADRH) was therefore urged to develop a data protection/privacy code of practice for digital identity schemes in Africa.

This book has therefore been developed with the direction, advice and support of various individuals and organisations. The Africa Digital Rights' Hub (ADRH) expresses its profound appreciation to everyone whose research, resources and time made this Code of Practice possible. We would like to especially thank the following:

- Omidyar Network;
- Our Founder & Executive Director - Mrs. Teki Akuetteh Falconer;
- The ADRH Team;
- G-Pak Ltd.;
- Ralph T. O'Brien, Principal Consultant, REINBO Consulting;

- Marie Penot, Founder & Consultant, EuroDataProtection, UG
- Emma Butler, DPO Yoti;
- Sebastian Manhart, COO SimPrints; and
- 2018 Data Protection Africa Summit Focus Group on Digital Identity and Addressing Systems in Africa.

2. DATA PROTECTION/PRIVACY IN AFRICA

Africa is undergoing a significant transformation and it is not in doubt that technology has played, and will continue to play, a major role in the process. It comes as no surprise that African countries have taken bold steps in the adoption, development and use of information and communication technologies (ICTs). In line with these changes, countries are also embracing policies and laws to facilitate the development and use of ICTs. Data protection and privacy laws are components of the legal protections that various countries are developing.

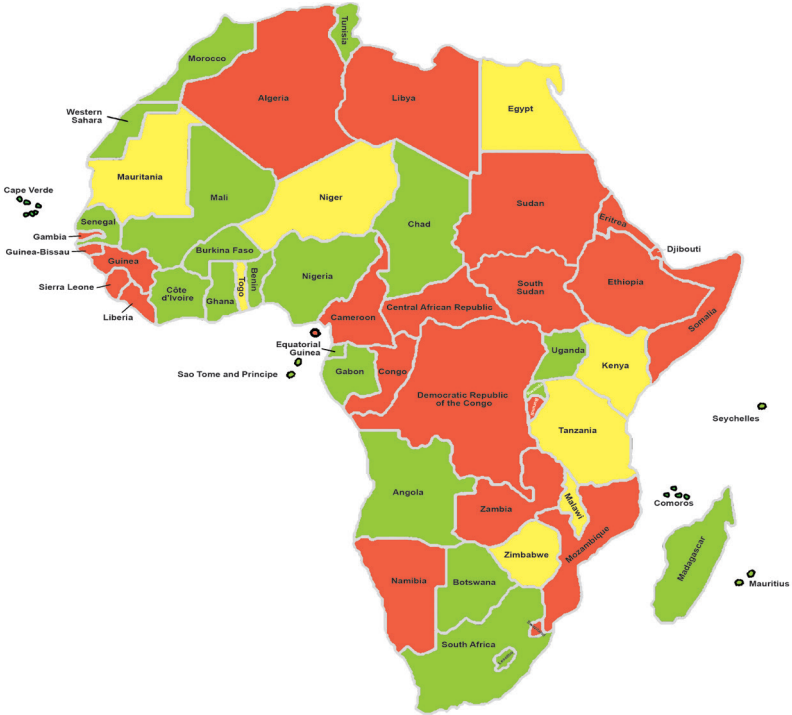
Data technologies have been evolving for over 100 years and protection and privacy requirements have evolved along with the progress of technology. Key landmarks in the field include: the first automated business data processing during the U. S. Census of 1890; the end of World War II; the Universal Declaration of Human Rights in 1948; the establishment of the basic principles of data protection by the Organization for Economic Co-operation and Development ("OECD") in 1980; and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (popularly known as 'Convention 108') by the Council of Europe in Strasbourg, France in 1981. And technology continues to be the trigger in the world of business data processing. The frameworks and laws of data protection are developed mainly in response to technological advances that increase the collection, holding and dissemination of personal information as well as surveillance.


Africa's data protection/privacy environment has been steadily growing over the past ten (10) years. Influenced by Europe's uniform approach that uses an omnibus law which governs all sectors and recognizes data protection/privacy as a human right,

the Continent's ecosystem can be described as underdeveloped and disparate in spite of some dynamic and progressive frameworks and laws.

At the continental and regional levels there are the African Union Convention on Cyber Security and Personal Data Protection (2014); SADC Model Law on Data Protection (2010); ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection (2010); and the EAC Framework for Cyberlaws (2008). Out of the fifty-five (55) African countries as at July 2019, twenty-four (24) have data protection laws with nine (9) having draft legislations at various stages (Table 1 below). Most of the countries also recognise the right to privacy as a fundamental human right under their respective constitutions. Of the countries that have data protection laws there are differences in the structures and approaches to implementation. These disparities in the various country laws are influenced by their legal, political, economic, cultural and societal systems.

Map of Data Protection / Privacy Laws in Africa (as at July 2019)



-  No data protection laws
-  In progress
-  Data protection law present

3. DIGITAL IDENTITY FOREWORD

The World Bank has noted that an estimated 1.5 billion people in the world today lack “legal identity”, meaning they do not have access to identification documents such as birth certificates, national ID cards or passports. In short, they cannot prove who they are.

Article 6 of the United Nations Declaration of Human Rights states “Everyone has the right to recognition everywhere as a person before the law” and accordingly part of the UN Sustainable Development goals (point 16.9) for 2030 - is “*a legal identity for all*”.

However, the deployment and management of identity schemes have been open to privacy abuses, with real world consequences for individuals. For example, denial of access to critical services (exclusion), identity-based discrimination, identity theft, surveillance, etc. It is important to note that no system of mass surveillance or data collection exists that has not been abused or used in harming individuals. Yet, societies continue to recognise and reap the benefits of large databases of personal information to create insights and provide services for the public good.

The challenge is to take advantage of the great benefits offered by the identity scheme technologies while minimising uses that abuse, discriminate (intentionally or unintentionally) or put at risk the lives and livelihoods of the individuals it intends to benefit or serve. Privacy is always a balancing act and new and innovative technologies always carry the risk of the unknown.

The current laws that ID issuers in Africa rely on in executing their mandate provide limited guidance on practical steps that can be taken towards respecting the fundamental right of privacy by individuals whose information they process. As a result, even where they claim legal compliance has been attained, individual empowerment (rights) are not necessarily guaranteed.

Building trust with transparency and accountability will only be achieved when ID programmes adopt a Code of Practice (COP) that incorporates steps that enhance privacy and data protection. This standard of compliance requires intentional practice that goes beyond the legal tools provided by various governments.

The Code of Practice (COP) will facilitate the adoption and implementation of good practices that ensure adequate protection and guarantee of the right to privacy of subjects of digital ID and addressing in Africa. As a guide to the adoption and implementation of standards and/or processes that assure good data protection practices for the development and use of digital identity schemes, it is a generic tool developed based on knowledge and appreciation of both the African landscape and international best practices. The Code of Practice is a useful guide/manual to policy makers, regulators, digital ID and addressing developers and implementors (both government and Private Sector) in Africa. It is a do-it-yourself guide towards achieving good IDs, applying a principle-based approach to privacy and data protection to the development and use of digital identity schemes for both commercial and governmental use.

While the COP cannot provide definitive answers in all cases it can serve as a “toolkit workbook” that gives organisations a structured approach to assessing the risks of harm and taking practical steps to reduce those risks.

No greater power can exist than the ability of an organisation or a government to determine, fundamentally, who someone is, and

therefore what they can or cannot participate in, what services they can or cannot have access to. The benefits to the individual can be empowering; the harms catastrophic. With great power comes great responsibility. It is critical that the Data Protection community in Africa gets this right, or we risk great harms to both the individual and to society as a whole.

4. ISSUES ON THE AFRICAN CONTINENT

LEGISLATIVE LANDSCAPE

The laws that govern identity schemes in African countries range from laws requiring the setting up national IDs, national health insurance schemes, social security and social protection schemes, etc. through to electronic transactions and data protection laws. The laws on data protection/privacy as mentioned earlier have been undergoing significant transformation. With the increase in the deployment and use of digital IDs in Africa by governments there have been more and more challenges and complaints on perceived data protection/privacy violations associated with ID schemes. Although many data protection authorities have supported identity scheme operations to facilitate compliance, they go on to face related challenges, including risks associated with sensitive identity data, biometrics and lack of capacity to effectively implement data protection/privacy compliance.

IDENTITY CRISIS

The United Nations has highlighted identity for Africa (ID4Africa) as one of its strategic development goals (SDG 16.9). This is a “movement that aims to help African nations achieve the objectives of SDG 16.9 by facilitating exchange of knowledge and expertise related to digital identity and promoting the development of principles and standards derived from real world experience in Africa.”

The UN Report identified that without effective identity management, the human rights of many individuals on the African continent would be violated or put at risk, these rights include:

- The right to vote
- The ability to earn or to keep a job
- The opportunity to attend school or university
- Travel across city, state, or national borders
- Government welfare benefits/services
- Police protection
- Government or employer pensions
- Healthcare
- Non-governmental organisation (NGO) aid
- Protection against illegal conscription into armies or militias

TAKING PART IN THE “FOURTH INDUSTRIAL REVOLUTION”

Africa cannot afford to be left behind in the “fourth industrial revolution”. And in order to benefit and promote growth and development of national economies as safe places to do business and attract investment, governments must address key concerns of this age. This means having interoperable standards in the digital space and equivalent laws that allow growth and development; facilitate investments; as well as build integrity and credibility into systems and processes; while safely ensuring the transfer and storage personal data. Today, on the continent, we can boast of several frameworks and substantive regional and country level laws that seek to address the issues of privacy and data protection as noted above. Most African countries with privacy/data protection laws have opted to pass general omnibus privacy/data protection laws based on human rights foundations that reflect the OECD and principles that form the foundation of privacy/data protection laws that have historically been developed and led by European countries.

NOBODY WANTS TO BE LEFT BEHIND

African nations and citizens cannot afford to be abused or taken advantage of, as has occurred in the past. With her positioning as the most highly resourced continent in the World today, Africa

must operate as an equal partner on the international stage for its development and growth. This means taking advantage of the opportunities new technologies bring, with proactive policy initiatives that evolve laws and regulations to manage the risks associated with them, and guard against the exploitation of individuals data in the rush to embrace new technologies.

NOT ALL ARE STARTING FROM THE SAME POSITION

There are huge variations in the economies that make up the African Union. Each country has its own priorities; legal systems and structures; differing levels of economic and social success; and levels of stability and security for its citizens. This means that not all starting points are equal, and priorities for some nation states will differ, as will their resultant approaches to privacy and data protection.

PRIVACY LEGISLATION AT PRESENT IN AFRICA

Several countries with privacy and data protection laws have regulators, but enforcement can be said to be weak or minimal compared to other regulators internationally. Often fines are criminal in nature, small, have to be awarded by expensive court action, with little or no powers granted to the regulator to impose their own administrative sanctions or fines. Without effective enforcement of such laws, many companies and governments can carry out non-compliant actions without consequences. In as much as enforcement of privacy laws are critical to the protection of individuals, it is important to recognise that the adoption of best practices is beneficial to all stakeholders especially industry and governments.

IDENTITY SCHEMES AT PRESENT

Many national ID card schemes have been initiated across Africa, and whilst some have failed, some are proving to be successful.

Notably Ghana and Kenya are still developing schemes that, at time of writing, are not fully rolled out. However, privacy issues are already emerging. For example, in a recent consolidated case brought by a number of entities including the Kenya Human Rights Commission, has challenged the alleged collection of DNA data for Kenya's national ID scheme, arguing that it infringes on the right to privacy. The court's temporary ruling held that, *"the inclusion of DNA as one of the unique identifiers or attributes in the definition of biometric in section three of the registration of persons act be and is hereby suspended pending the hearing of the consolidated petitions."* The court's ruling also barred the sharing of information on the system with third parties — including other government agencies. Internationally, some of the very successful identity schemes, such as the one in India, have also recently come under judicial scrutiny (mostly from the Supreme Courts) based on concerns surrounding the protection of the fundamental rights to privacy.

5. ID SCHEMES

STAKEHOLDERS

The stakeholders in any ID scheme are critical to the success of the scheme and have varied roles to play. Below are the list of the key stakeholders and the roles they play.

Individuals

Individuals are the end-users of identification systems. The proof of identity the systems provide give them access to services and a range of rights. The rights they are guaranteed under privacy/data protection laws include the right for the processing of their data to be made transparent. They should be empowered to exercise appropriate control over how their data is collected, used, stored, and shared.

Governments

Government agencies are the usual providers of legal identification systems. A legal ID issued by a government may be analogue or digital. When digital, that may include IDs that use biometrics, smart cards, PIN, tokens, magnetic strip, or QR code. A government issued ID may also take many forms, including foundational ID (possibly a national ID) or functional ID for a specific purpose such as voting, access to a safety net program, school, health care.

These include, but are not limited to, civil registers, including birth, death, and marriage registration, population registers, national IDs, passports, voter registers and cards. Government agencies are also users of identification systems for programme

administration functions such as social protection programmes, tax collection and providing licenses.

Private sector

Private companies are the main developers, innovators, and suppliers of identification system technology infrastructure. The relationship between governments and private companies is symbiotic as many private companies also rely on legal identification systems to identify the customers who access their products and services. Governments have also partnered with private companies to deliver forms of identification—such as mobile identity and digital certificates—that expand the reach and utility of legal identification systems to individuals.

International organisations and NGOs

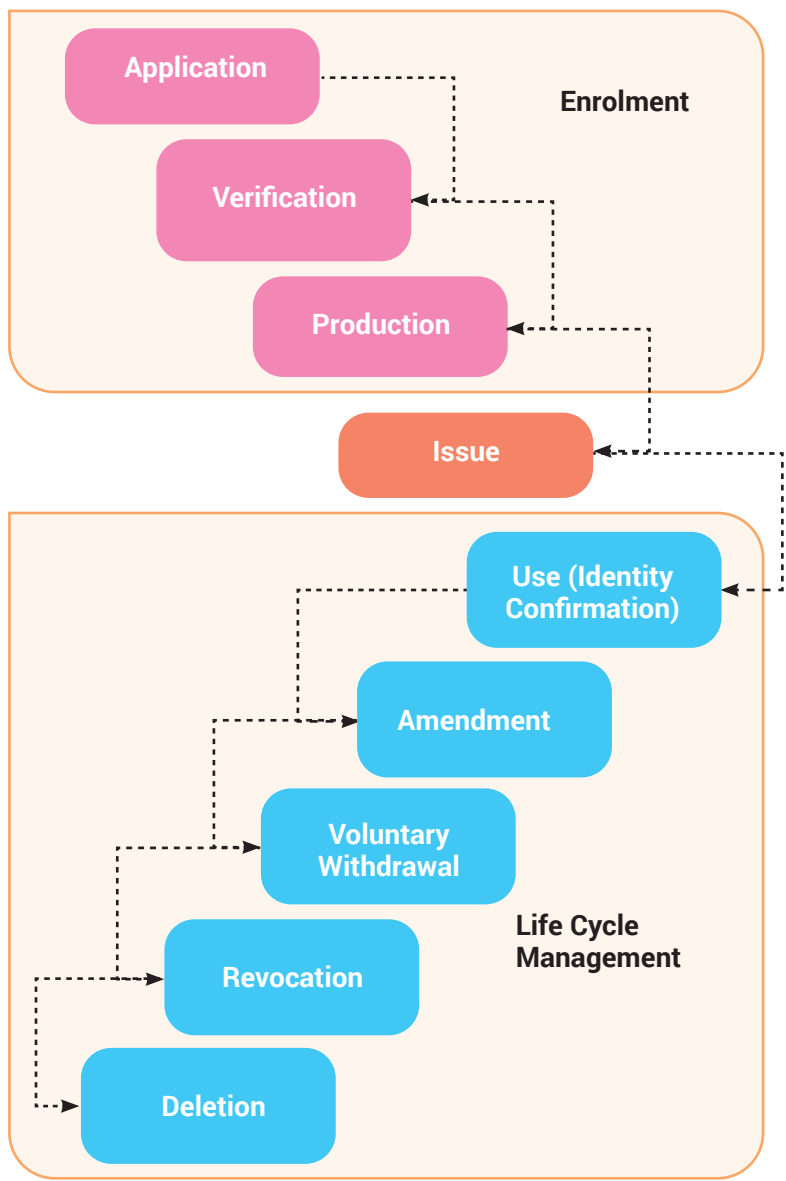
Mostly made up of civil society organisations, they usually manifest the interest of individuals, citizens or specific groups. By providing pressure, lobbying, legal intervention, legal assistance and other services. International organisations, civil society and community organisations are important stakeholders in the generation, demand for identification and assisting people in accessing the identification they need to fully engage with society.

Development partners

Development agencies, other donors, and humanitarian organisations can provide support for identity schemes in the form of funding and technical assistance and may also operate their own identification systems to administer programs.

ID SCHEME LIFECYCLE CONSIDERATIONS

The following terminology is used to describe the operation of an ID scheme.



Application

Where the individual applies for an ID.

Verification

Where the individual's application is reviewed for accuracy and verified.

Production

The production/manufacture of the ID.

Issue

The transmission of the ID to the individual.

Use (Identity Confirmation)

Usage of the ID to verify the individual's identity.

Amendment

Amendment of the information on the ID where the individual's information has changed or is found to be inaccurate.

Voluntary Withdrawal

Where the individual chooses not to be part of the ID scheme and withdraws.

Revocation

Where the ID is removed or taken from an individual for a valid reason.

Data Retention/Deletion

Where the data on the individual is kept for a period of time before being destroyed.

6. ARGUMENTS SURROUNDING ID SCHEMES

TYPES OF IDENTITY SCHEME PROVIDERS (IDSP)

This document refers to the operators of identity schemes as Identity Scheme Providers or IDSP. These may be private, public or government operated schemes; and this document aims to equally apply to all schemes, no matter the type of organisation running the programme.

Types of Identity schemes

This Code of Practice is designed to apply across the full range of identity schemes, some examples of these schemes include:

- Service specific such as passports, licences, etc;
- Private Identity card schemes;
- Digital Identity schemes;
- Age verification schemes;
- Government ID schemes; and
- National ID cards such as in Ghana, SA, Nigeria, Kenya.

DANGERS SURROUNDING DIGITAL ID SCHEMES

Unfairness

Discrimination against certain groups is always a concern when factors relating to their address, ethnic grouping, gender, tribal origin or sexuality come into play. It is a logical concern then, once ID cards are in place whether these become mandatory to carry. This can heighten the inequalities that already exist e.g. ethnically biased “stop and search” practices. ID cards could

eventually become an internal passport, carried by anyone who might face questions about their immigration status.

Expensive

It could be argued that the resources required to roll out an ID scheme nationally would be far better spent ensuring agencies such as the police are better equipped. If it is proposed to levy a charge that individuals would have to pay to replace lost cards, or change personal details when moving house or changing their name, the scheme risks excluding people with lower incomes. If fines are levied on people who do not notify the authorities of changes in personal data, these schemes could further criminalise individuals for simple administrative lapses.

Intrusive and unsafe

Large amounts of information (including former addresses and immigration status) can be held about individuals in the ID, with the likelihood of more being held in the future. This information could be shared with many agencies within governments, but also non-governmental sub-contractors with scope for extension into the private sector. Recent high profile losses of sensitive information raise doubts about the ability of governments to manage so much information securely, and the schemes would certainly be a target for anyone looking to commit offences.

Inclusion vrs. Exclusion

It has been established that whiles ID schemes may be beneficial in identifying particular groups of persons for the purposes of providing them with the services they require, the challenges around enrolment and access may sometimes lead to discrimination and exclusion of individuals and or certain communities.

7. ORGANISATIONAL ACCOUNTABILITY

IDSPs should ensure they are in a position to proactively demonstrate compliance with this code of practice, international commitments and obligations, and national laws. Accountability means that IDSPs have a responsibility to keep detailed records of how they manage the data of individuals in order to prove that they are in compliance with the laws, standards and regulations that apply to them (including this code of practice).

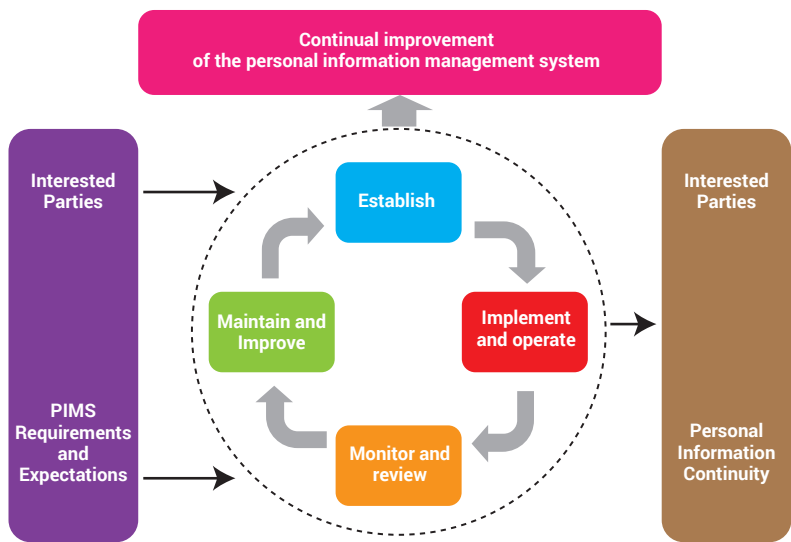
This strategic top down approach to privacy management also satisfies the accountability principle (see next section) of legal requirements. Each data flow or business unit should look at using the remaining privacy principles tactically to address each data flow or use of personal data.

High levels of accountability are critical to ensure that IDSP have planned, delivered and applied relevant and correct controls to manage the risks to individuals.

PRIVACY MANAGEMENT

The organisation should adopt a continual improvement approach to establishing, implementing, monitoring and improving a Privacy Management System as part of its wider business management system on a continual basis. Standards such as BS10012:2017 and ISO 27701:2019 are designed to allow organisations to achieve externally and independently assessed accredited certification for a Personal Information Management System, to prove, externally, they have put in place a set of controls to manage individuals data.

TABLE 2 - Privacy Management Cycle



PRIVACY EXPERTISE

IDSP should not attempt to create and maintain an IDS without appropriate access to privacy advisory resources. This could be internal expertise, or expertise sourced from external resources. There are several roles and responsibilities that should be adopted with a privacy element to their role.

These roles can include:

- Senior accountable officer: responsible for privacy management, should be a senior management role.
- Data Protection Officer; Audit and review role, “voice” of the individual within the organisation.
- Privacy risk manager: responsible for managing risk to the individuals and reporting on how these risks are managed.

- Privacy Programme manager: responsible for establishing and implementing the privacy programme within an organisation.
- Privacy manager: responsible for day to day running and maintenance of the privacy programme, such as providing advice to the business, and managing documentation and records, possibly responding to individual requests.
- Privacy audit and review: responsible for identifying improvement opportunities and assessing the privacy programme against identified requirements.
- Privacy Legal expertise: advisors on legal requirements and national law compliance.
- Privacy Engineer: privacy by design expert, normally within software development and solution design.
- Privacy Consultancy: extensively experienced (normally 10 years +) advisors that guide organisations building privacy programmes.

PRIVACY BY DESIGN

Privacy should be a forethought not an afterthought. This code can be used both as a check to ensure that the relevant privacy principles have been considered in advance. The principles can then be factored into the requirements for system design, development or purchase, and passed on to any relevant third party organisations. It is far easier to factor in privacy proactively than try and retrospectively bolt on features once the system is in operation. Before operation, checks should be made against the requirements identified in the design phase to ensure that they have been fulfilled in development.

By using this code, an IDSP can use the “boxed text” surrounding any proposed solution in order to prove and carry out an audit to identify privacy requirements appropriate for their ID solution, thus fulfilling the privacy by design requirements of an IDSP.

PRIVACY BY DEFAULT

Where choices can be made by individuals regarding the use of their data, and options can be exercised by the individual, the scheme should be designed in such a way that the default choices are set to the most privacy protective. This allows individuals to “opt in” to elements such as data sharing, rather than having to “opt out” of these settings.

Opt-In vs Opt-Out

The image shows four examples of user interface prompts for marketing preferences, illustrating the difference between Opt-In and Opt-Out. Each example consists of a text prompt, two checkboxes, and a green or red checkmark indicating the best practice.

Text Prompt	Checkbox 1	Checkbox 2	Indicator
Would you like some marketing options (No options pre-ticked)	<input type="checkbox"/> Y	<input type="checkbox"/> N	Green checkmark
Would you like some marketing options (Pre-ticked)	<input checked="" type="checkbox"/> X	<input type="checkbox"/> N	Red X
Please send me some information (Pre-ticked)	<input checked="" type="checkbox"/> X	<input checked="" type="checkbox"/> N	Red X
Tick here if you DO NOT want additional marketing (Opt - Out)	<input type="checkbox"/>	<input type="checkbox"/>	Red X

Current best practice is to allow users of systems and software a “user self-service” design, where they can access their privacy preferences and exercise their rights themselves, without having to resort to manual processes.

PRIVACY IMPACT ASSESSMENT

The IDSP should complete and document a Privacy Impact Assessment to record the privacy risks to the individual, and the measures that have been implemented to manage these risks.

The Privacy Impact should include:

- ☐ A description of the data to be processed
- ☐ A description of the individual whose data will be processed
- ☐ A description of the processing, including a timeline of the data from collection to disposal
- ☐ A description of the risks the processing causes to the individual
- ☐ A description of the measures applied to manage the risks
- ☐ A description of the legal requirements that apply
- ☐ A description of the advice given during consultation with regulators
- ☐ A description of advice given by privacy expertise and regulators
- ☐ A description of the consultation carried out with individuals, and their views gathered
- ☐ A description of the measures applied to comply with the advice given
- ☐ A description of any residual risks, or measures that could not be managed or implemented and the justification and acceptance of management for these.

RECORDS OF PROCESSING

An organisation should make a record of its processing operations in order to establish the information relevant to the processing of each individual's data along its data lifecycle. All points of the data lifecycle should be recorded including privacy relevant metadata surrounding the data itself, individuals, purposes, secondary purposes, collection, storage, access, transfers, third party involvement, security, disclosures, retention and disposal. The record of processing activities should be kept up to date

throughout the operation of the scheme, and any alteration to the processing activities of the scheme should be reviewed for privacy risks.

This is a significant project in itself, and examination resourcing should not be underestimated. It will form the foundation of understanding of both the personal data processed, and the controls to protect it. It is recommended to look at data movement throughout its lifecycle, from collection, through to use, storage, secondary use, transfers, and ultimately its retention and deletion. Gathering the data here will be useful in order to understand and control the processing, understand risks to the individual and the organisation and any relevant risk mitigation techniques that can be brought into play, such as data minimisation, encryption, anonymisation, obfuscation etc. These records of processing will need to be maintained and updated as processing changes throughout the operation of the IDSP.

At a minimum the following data should be collected as part of the records of processing:

- **Collection**

- ☐ Privacy notices
- ☐ Personal Data types collected
- ☐ Types of Individual (especially children and vulnerable groups)
- ☐ How is it collected, who from?
- ☐ Special Category data
- ☐ Special Category legal basis
- ☐ Minimisation techniques
- ☐ Anonymisation techniques

- **Use**

- ☐ Purposes
- ☐ Legal Basis
- ☐ Minimisation techniques
- ☐ Anonymisation techniques
- ☐ Controller or processor status
- ☐ Additional data added or derived from the data

- **Storage**

- ☐ Formats of data
- ☐ Locations of data storage and transfer
- ☐ Appropriate Protection and security methods
- ☐ Third party involvement and contracts
- ☐ International transfer and justification
- ☐ Data Subjects Rights and access to data

- **Secondary Use**

- ☐ Secondary purposes
- ☐ Legal basis for use
- ☐ Retention period
- ☐ Data minimisation strategy
- ☐ Anonymisation techniques

- **Access, Transfer and Disclosures**

- ☐ Groups with Access to data
- ☐ Security and authentication
- ☐ Amount of data disclosed
- ☐ Data extracts taken and extract control
- ☐ Third parties and contracts
- ☐ Recipients
- ☐ Justification
- ☐ Amount of data transferred

- ☐ International transfer and justification
- ☐ Appropriate security and protections

- **Retention**

- ☐ Timescales
- ☐ Justification
- ☐ Purpose of retention
- ☐ Weeding

- **Deletion**

- ☐ Secure deletion methods
- ☐ Disposal vs retention schedule

SUPERVISORY AUTHORITIES AND CONSULTATION

Before operation of the scheme the IDSP should enter into consultation with an appropriate supervisory authority, disclosing all of their records of processing, privacy impact assessments and other relevant information surrounding the operation of the scheme and should incorporate any commentary and recommendations that it has.

In addition to this, further consultation should be carried out amongst a sample of individuals to be subject to the scheme in order to seek their views on the processing and incorporate their views into the final operation of the solution.

Supervisory authorities may be sectoral (for example in the healthcare sector) or a privacy regulator in themselves. African Privacy regulators can be found listed by country in Appendix B.

BREACH NOTIFICATION

In addition to a comprehensive set of security controls that are appropriate to the security risks faced in the environment, preparation should be made to detect and respond to any breach of confidentiality, availability and integrity of the individual's data held and processed by the scheme.

The breach notification process should include roles and responsibilities, reporting lines and timelines, escalation points, and lines of communications to be carried out upon discovery of a breach, along with steps to identify and remediate any damage caused. IDSP should stay informed of any legal responsibilities they may have to report to appropriate regulators or individuals themselves.

THIRD PARTY MANAGEMENT

Most IDSP will rely on third party technology providers in order to assist them with the delivery of their scheme. In each case the IDSP should carry out appropriate due diligence, contractual measures and monitoring of the third party providers to ensure compliance.

Due Diligence should include:

- ☐ Certifications
- ☐ History of incident
- ☐ History of regulator investigation
- ☐ Stability

Contractual Measures should include:

- ☐ To process only on the IDSP instruction
- ☐ Staff committed to confidentiality measures

- ☐ Adherence to specific security control requirements defined by the IDSP
- ☐ Only to engage another sub-processor with written permission of the IDSP
- ☐ Assist the IDSP with their compliance and responsibilities
- ☐ Delete or return the personal data at the conclusion of the contract
- ☐ Make available all information necessary to prove compliance
- ☐ Open themselves to audit and review of their processing activities

Contractual Monitoring should include:

- ☐ Variation according to the risk posed by the third party processor
- ☐ Submission of operational performance statistics and measurements
- ☐ Regular review meetings
- ☐ Third party Certifications
- ☐ Audits and assessments

CODES OF CONDUCT AND CERTIFICATION

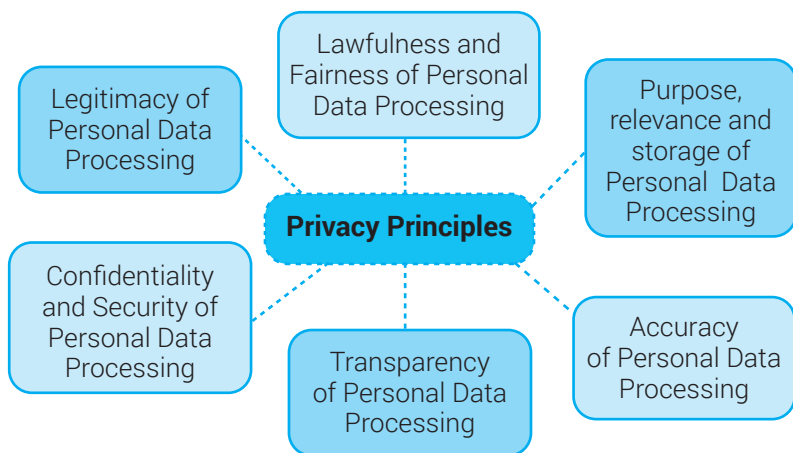
The IDSP should identify relevant standards and codes of practices that may be relevant to their processing activities and use these codes of practices as an aid to identify relevant controls in order to protect the individuals their schemes serve. In addition, they should review available independent accredited certification schemes for applicability and hold and maintain relevant independent accredited certification in order to provide assurance of their compliance.

MEASURING MONITORING, AUDIT AND IMPROVEMENT

The IDSP should identify areas where the privacy risks and controls can be monitored and measured in operation, to ensure a level of control that is appropriate to the risks. This may and should include external and internal independent audit to identify areas of non-compliance and improvement opportunity within the operation of the scheme, and the IDSP should take and document appropriate corrective and preventive actions to ensure these identified actions are carried out and are effective.

8. PRIVACY PRINCIPLES

Most of the data protection/privacy laws currently have similar principles. For purposes of this document we will place emphasis on Article 13 of the Malabo Convention of the African Union on Cyber Security and Personal Data Protection which contains the following principles that can also be identified in most of the regional and country texts or laws:



The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980 (revised in 2013) have also remained the cornerstone of good privacy practice. Most data protection and privacy laws across Africa have been influenced by the OECD principles as well as their European counterparts. Today, the GDPR (General Data Protection Regulation) of Europe is often regarded as the most advanced privacy/data protection law in the world, and the one that most organisations aspire to as a “Global Gold Standard” and thus the main body of this Code of

Practice also takes into consideration these principles to the work of IDSP, and should be considered a guide to good practice.

Conventions that operate and have received agreement across various African states include, Convention 108 (and Modernised 108+), the Malabo Convention, ECOWAS Directive and SADC model laws. These conventions and the existing privacy or data protection laws in Africa have also been taken into consideration in the development of this Code.

This section is organised with a discourse on each topic, followed by “boxed text” that can be used as a “checklist” to ensure an IDSP is applying the appropriate privacy management to their scheme.

LEGITIMATE LEGAL BASIS

Personal data must not be processed without a lawful justification for doing so. In most legal regimes, there is provision for categories of legal basis that can be selected to make the processing of personal data valid, and in most jurisdictions certain types of data are considered “sensitive” or “special category” and should seek further or more specific legal basis in addition in order to be processed by the IDSP.

Special Category Data

Though legal definitions vary from jurisdiction to jurisdiction, the following data types are often considered more “sensitive” and may require a secondary justification or legal basis in order to legitimise the processing:

- Physical or mental health or wellbeing
- Political views or affiliations
- Religious beliefs or others of a similar nature
- Trade union or Political pressure group memberships
- Biometric identifiers (such as fingerprints, iris scans etc),

- DNA or other genetic information
- Racial, Ethnic or Tribal origins/affiliations
- Sex Life, Sexuality and sexual activities
- Alleged or actual criminal or civil offences, and their disposal in a court of law
- In some jurisdictions financial data is considered special category data
- In some jurisdictions government ID numbers themselves may be considered special category data

Mandatory vs Optional schemes

It is worth noting there is a gulf of difference between optional commercial schemes (that individual's may or may not join with consent of commercial contract), and mandatory schemes enforced by Governments. The latter require individuals to join in order to access a service and they normally require legislation to enable their enrolment. For eg. licensing, passports, citizenship, identity cards, etc.



Note 1: Multiple legal basis for processing personal data exist, but each should be narrowly applied such that different purposes of uses for the same data will each require individual justification. For example, data gathered for one purpose, but subsequently used for another should have a valid legal basis for both uses of the data.



Note 2: Equally, there may be some data gathered under one legal basis (such as data deemed mandatory under legislation), and other data also gathered that may be discretionary to give (justified only by the consent of the individual). In these cases the difference should be made clear to the individual at the time of collection. For example, though name and address may be mandatory for the IDSP to operate, the use of an email address for direct marketing may be optional and consent based, and should be made clear to the individual.

Legal basis that can be chosen may include the following:

Legislation, or a legal obligation that requires an IDSP: Where the IDSP is a government organisation, they may pass specific legislation to enable their scheme, but this legislation should not enable any collection that breaches any of the principles outlined in this section.

Consent of the individual: Where consent is relied upon it should be Informed (so individuals understand the full scope of what they are agreeing to), freely given, specific, be able to be evidenced and must be a positive affirmative action taken by the individual. Where consent is relied upon the individual must be able to withdraw the consent as easily as they gave it. Consents should be narrow, giving individuals the maximum amount of choice in the use of their data.

Contractual Necessity: Normally where a commercial entity wishes to provide entity management in order to facilitate a contract, or prove entitlement to gain access to a product or service. In this case care should be taken to ensure both purpose

limitation and collection limitation to strictly that minimal data necessary for the operation of the contract, and seek other legal basis for other optional uses.

Public interest: Where there may be overwhelming societal reasons for such a scheme that outweighs usual individual privacy rights. Examples could be at a time of national crisis, warfare or public health, where individuals may pose a danger without proper identification and control. Where Public interest is claimed an assessment that justifies how the public interest outweighs the individual right to privacy must be carried out, and should have documented the appropriate protections and safeguards applied within the Data Protection Impact Assessment (DPIA).

- ☐ Identify and Document all legal basis for processing, considering the strengths of each; this may include a Legal Obligation, Contractual necessity (strong), Public/ Legitimate/ Vital interests arguments (arguable) or Consent (weak)
- ☐ Ensure all purposes of processing have a legal basis
- ☐ Identify and justify the use of sensitive or special category data
- ☐ Identify where data is mandatory to supply and where optional
- ☐ Ensure where different legal basis are used this is made transparent,
- ☐ Ensure individuals are told how this may affect their choices and rights
- ☐ Make sure "sensitive" or "special category" data types are identified and alternative legal basis justified where necessary
- ☐ Where relying on Consent ensure this is freely given, granular/specific, informed, documented and a positive "opt in" by the individual

PURPOSE LIMITATION

Primary Purposes of use

Naturally the data will be collected for a lawful purpose to carry out the IDSP. This is referred to as the “primary purpose” of collection. This purpose needs to be identified, documented and a legal basis chosen as above. However, one of the fundamental risks to individuals with ID schemes is “scope creep” or “function creep”, where data collected for one purpose is used for another. Therefore strict limitations on what the data can be used for are required, and any secondary purposes that the data may subsequently be used for should be identified prior to operation.

Secondary Purpose of use

Prior to the operation of any ID scheme, thought must be given to other uses of data beyond the obvious primary purpose of the scheme. For example; data taken in order to allow an age verification card scheme, may subsequently be used for statistical profiling of its users, and then again sold on to third parties to target advertisements at them. Similarly, information gathered for a national identity card could be used to ethnically profile or send political messages to individuals. Equally, this information may also be accessed and used by law enforcement. All of these proposed secondary uses of the data need to be identified before scheme operation, and purposes should not be “bundled” with “enforced consent” so that an individual cannot refuse something where they should have genuine choice over the secondary purpose of data use. Remember to include data uses that are ancillary, such as security, research and development and monitoring.

New Purposes

Once the scheme enters operation, often the purposes change or the data is requested to be used for new purposes not originally identified. IDSP should be especially careful to limit this and manage it carefully, ensuring that any new purpose has

a valid legal basis. In any case the new purpose needs to be communicated and transparent to the service user, unless a legal exemption applies. Where the legal basis relied upon gives the individual choices these should be clearly indicated and easy for the individual to exercise.

Third party usage/connections

Also identify purposes of data use that may be conducted by third party organisations with access to the data, including service providers who assist in the operate the scheme. Make sure in third party contracts it is explicitly spelled out that they cannot use the data for other purposes than those directed and instructed by the IDSP.

- ☐ Identify the primary purposes of processing
- ☐ Identify any secondary purposes of processing
- ☐ Identify the minimum data required for each purpose
- ☐ Ensure a legal basis for each purpose
- ☐ Where purposes have genuine choices, these should not be hidden, be easy to exercise, and should not be bundled together with other data uses or consent assumed by accepting other data uses
- ☐ Ensure you are transparent about the uses of data with individuals
- ☐ Identify any uses of data by third parties and vendors
- ☐ Update contracts to ensure service providers are similarly limited on purpose of use throughout the supply chain
- ☐ Ensure no data uses occurs for subsequent purposes that has not been authorised or justified
- ☐ Where consent is revoked or no legal basis applies, ensure data is removed.

COLLECTION LIMITATION

In general, the amount of data collected must be the minimal possible to achieve the stated purposes. However it should be equally recognised that not having enough data to make appropriate decisions can be just as damaging to individuals (consider allergies in the medical field where not having data on hand could cause adverse reaction). In general the principle should be to find the minimal amount of data required to effectively achieve the goal of the IDSP, and not to collect superfluous or additional data "just in case" it becomes useful. This also extends to metadata, such as usage data on the scheme's operation itself. In addition to collection, along the data timeline this should also be considered in disclosures or access to data, where data access or transfers to others should be the minimal necessary to achieve the purpose, for example, sending single records instead of the whole data base, or only the specific fields required in order to achieve the purpose.

Where data collection is mixed between optional and mandatory, make sure this is made clear to the individual, so that data is not collected for purposes where they have decided not to participate. Equally, when Consent relied upon is revoked, data must be removed if no other legal basis exists to continue to process it.

There are several techniques that can be of use in minimising data and these include the following:

- **Anonymisation**

The ultimate way of minimising data is to consider whether the purpose can be achieved by removing all identifiability, meaning effectively that the data would fall outside of privacy law as it no longer poses any risk to the individual. However, it should be remembered that Anonymisation is not an absolute state, and that the removal of data reduces its utility and usefulness and

fitness for purpose. However, the more data included, the higher the likelihood or risk of the individual being able to be re-identified from the data, either by a small statistical group, or being able to be combined with other data that may be available publicly or privacy.

- **Pseudo – Anonymisation**

Pseudo anonymisation refers to the process of anonymising data to some parties, but leaving the identity recoverable by other parties. For example, you may have a third party provider who you wish to keep identities clear from, but enable yourself to see the identity – this is often achieved by removing identifiers and replacing with unique identifiers. It is important to note that though the data is no longer “identified”, it remains “identifiable” and therefore legally remains personal data.

- **Through life Minimisation**

Minimisation is not just surrounding collection, but at all stages of the information lifecycle. This includes the addition of additional information, other purposes of collection, access control to authorised individuals,

- **Systems Design**

It is important to perform privacy by design techniques to ensure supporting systems and data bases minimise the data stored. For example the use of “free text” field encourage extra, uncontrolled collection. Consider instead utilising categories, drop downs and character limited fields that will increase accuracy, increase efficiency, and reduce data collected – this should be an important consideration within the Privacy by design process.

- **DNA/Biometric data**

Some recent moves in the field of national ID cards have included collection and storage of DNA, genetic or biometric identifiers. It is important to note that an individual's DNA and Genetic code does not only reveal one's own code, but potentially that of his or her family too and should be carefully justified as to its necessity if it is to be collected. Similarly where biometric data is collected, care should be taken to minimise what data is used to identify individuals. A model that has seen some success is to "hash" fingerprint data into a shorter code that cannot be used to recover the original, and when compared to a fingerprint reader, to perform similar operations to see if the stored hash and the hash of the presented fingerprint match. That way no actual fingerprint data is required to be stored.

- ☐ Collect the minimum amounts of data to achieve the schemes' purpose
- ☐ Where secondary uses are in place, make sure that any optional data collection is made clear to the individual
- ☐ Make sure data access is the minimum necessary to internal and external recipients
- ☐ Make sure data transfers and disclosures are the minimum necessary to third parties and service providers
- ☐ Consider if the processing requires identification of individuals, and if not, remove identifying information from the data, or apply anonymisation techniques to the data
- ☐ Remember that anonymisation may reduce data utility, and there remains a risk of re-identification.
- ☐ Contractually enforce the behaviour of third parties to not attempt to re-identify individuals from anonymised or pseudo anonymised data

- ☐ Use privacy by design to develop systems that collect minimum data required.
- ☐ Where consent is revoked, or no legal basis applies, ensure data is removed.
- ☐ Consider using “hashed” data techniques so as to not store original fingerprints, passwords, iris scans etc.

FAIR PROCESSING, PRIVACY NOTICES AND TRANSPARENCY

Critical to privacy concerns is the need for Transparency with the individual. Regardless of whether they have choice or the scheme is mandatory, it is critical for individuals to understand all the circumstances of processing to enable them to understand the data usage, purposes of processing and be clear on what options and rights they may have. Full transparency is key to the individual understanding of the ID scheme, as is providing them with as much control over their data as possible.

Notices

Privacy notices are the mechanism most organisations choose to be transparent with the individuals. They should be given at the point of collection to ensure the consequences of the processing are transparent to the individual before collection and processing commences. Notices will be numerous in nature, and may be given in stages – for example data collection on mobile apps, paper based, telephony may all differ in the type and style of notice, as the data collection and processing will differ. Notices can include, verbal recordings, call centre scripts, notes on application forms or online text. In each case, care should be taken to ensure these are written in plain text for the target audience so to be easily understandable (i.e. not in produced in “legalese”), and longer and more complete privacy notice are available in FAQ style for those

that have any further queries. Put simply, the right information, at the right time, for the right people.

- ☐ Provide notices at points of data collection
- ☐ Review notice content for different collection channels, such as Text, Apps, Websites, Telephone, and Longer form FAQ style notices.
- ☐ Ensure notices are written in plain language, and made available free of charge and prominently
- ☐ Note that consents cannot be valid if the individual is not informed as to the entire nature of the processing
- ☐ Review information when processing changes
- ☐ Ensure that the notice covers the whole supply chain
- ☐ Provide and communicate further privacy notices if the processing and purposes change
- ☐ Privacy notices should contain information on:
 - Details on the IDSP identity including contact details
 - Details on privacy team contact
 - The purposes of processing
 - The legal basis for each purpose
 - If the legal basis is based on legitimate interests, a description of them
 - Any recipients or disclosures of the information
 - If transferred internationally, to where and under what justification
 - The retention time
 - Existence of individual rights and how to claim them, including how to complain and to any supervisory authority
 - How to withdraw consent where relied upon

- If the legal basis is a legal obligation, what this is
- The presence of computer based algorithmic decision making, and the consequences of this

Updating of notices

Obviously as soon as processing changes, privacy and transparency notices should be updated and altered as appropriate. This includes any processing changes from suppliers and subcontractors.

DATA QUALITY

The design of collection and systems architecture should allow for complete accuracy with personal information. Not only to establish confidence in the veracity of identity verification, but also protection of individuals involved in the scheme.

Design

Systems and Information collection mechanisms should ensure high data quality by ensuring that the data collected is limited. For example, rather than adding “Free Text” fields, categories can be used to ensure a limited options in data processing. Field integrity and data capture/input limitation and integrity checks can be used as limitations – for example, not allowing individuals to put 32 in a day field or 13 in a month field.

Verification

Checking data against common formats and other systems and established databases can be a useful way to verify the completeness and correctness of data. For example telephone numbers have common formats and can be verified against

providers where appropriate, however care should be taken against over sharing with other entities or forming combined databases with excessive data collection and use.

Changes

People change, and so does their identity data, births, deaths, marriages, changes of names, genders, addresses, contacts etc will mean that the data and identity information is a constantly living thing – and once data is collected, significant resource must be sent to ensure it remains up to date and accurate. This can mean links and further verification with other sources, or a secure user self-service model to allow updates. This may mean card or token re-issue to individuals. Remember that individuals can lie, and that fraudsters purposefully look to attack identity databases so changes again should be verified against other sources where appropriate.

- ☐ Ensure information collection forms allow for simple validation and verification checks.
- ☐ Use common formats and data integrity verification to ensure correct capture of information.
- ☐ Ensure that individuals can apply or gain secure access to change their data.
- ☐ Verify data against other sources where appropriate.
- ☐ Use common formats of data to ensure data accuracy.

STORAGE LIMITATION, RETENTION AND DELETION

Personal data has a lifecycle – and one of the most important elements of the lifecycle is its eventual deletion. Most laws state

that data should be deleted where no longer necessary for the purpose. Equally there may be other legal statutes that require data retention for specific periods – these obviously take priority and therefore legally required data retention is a mandatory requirement.

The deletion should be done at the information level, not at the whole record level- Weeding of the data may be just as appropriate, as some information within a record may have gone past its retention period or be no longer necessary to be retained, and others may still be valid to hold.

Security is also required in the Deletion of information, for all copies, in all places of storage.

- ☐ Identify the purposes of data use, and the appropriate retention periods for the data.
- ☐ Identify any legally mandated retention periods.
- ☐ Draft a retention schedule and ensure that it is implemented.
- ☐ Ensure the minimum amount of data is retained, weeding any information with a record that is beyond its purpose.
- ☐ Ensure deletion occurs across Data backups, copies, third parties and archives.
- ☐ Ensure data destruction methods ensure secure destruction.

INDIVIDUAL RIGHTS

Individuals are granted rights by law and also, should have the opportunity to exercise their choices where applicable, or where the law requires organisations and IDSP to provide them for the individuals they serve. Systems should be designed with these

rights in mind, and as part of systems design facility to enable these rights should be built in. To reduce overheads on the IDSP, often a self-service model can be employed, with the individual gaining these options via automated solutions, rather than via manual request. However, manual options should also exist, to facilitate rights for those without access to technology. These include rights to being given access to copies of the information that an IDSP holds itself – these rights can include;

Access

The right to have a copy of all information held by an IDSP. This includes having a secure method to authenticate the individuals requesting the information, and to send the information via an appropriate secure channel to the individual requesting it. Legal rights may specify a time period for response, and possible cost an IDSP can charge, whilst other jurisdictions allow this right for free. This may also include a right to other information surrounding the data, such as disclosures, recipients, purposes of use, retention periods, international transfers, etc. This right is essential, because without understanding the data held, it is unlikely that the individual will be able to pursue the additional rights below.

Erasure

In some jurisdictions a limited right exists to request data deletion, however this normally only applies where the organisations do not have the legal basis to keep holding data (such as where relying on a consent that has been withdrawn), or where the organisation has broken these privacy principles (for example, retaining information past its retention period, or holding excessive or unnecessary data).

Rectification

Where information is incorrect, individuals should be in a position to correct it. However, this should not happen without proof of the veracity of individual's claim. Equally, where an individual has asked for data to be corrected or changed and the IDSP has been unable or unwilling to comply due to a disagreement, this should be noted and logged.

Objection

Where data uses are optional, individuals should be provided with clear ways to ensure their data use preferences can be taken and respected. This includes objection to purposes that are not mandatory for the scheme, such as data uses for marketing, research, statistics, public interest or anything based on a balancing test surrounding individual's rights.

Restriction

Whilst disagreements exist between the IDSP and the individual, it may be that continued use of the data may place the individual at risk, and the individual should have the right to request that data is set aside and marked "do not use" for the duration of the disagreement, or until the risk to the individual has passed.

Portability

Some jurisdictions allow individuals to ask (where the legal basis is consent or contractual necessity) to transfer the data they have submitted (not any data the IDSP has added) to a new provider. This information should be made with interoperability in mind in order that common formats can be used to transmit the data to other providers in formats that are easy for them to utilise.

Automated Decision making

As in the transparency and notice section, individuals must be informed when computer based algorithms make judgements or decisions about them according to some criteria – with identity management, this could mean that computers are making comparisons in order to grant access to their authentication for example. Individuals should be granted some understanding of the logic behind the decision making process, and have the right in some jurisdictions to have this decision re-evaluated by a human being. These rights have not historically seen much use, but it is envisaged as computers increasingly make decisions for us based on algorithms, this is an area in which individuals will be increasingly trying to utilise their rights.

Lodge Complaint/Remedy

Individuals should be given facility to raise any concerns they have with the IDSP, and effective dealings with the individuals at this time can prevent the individual from escalating their complaint to a regulator or a court of law. Dealing with individuals fairly and efficiently and giving them transparent access and swift remediation to problems with their data should be a key line of defence to allow IDSP to be able to gain an early warning of future problems and deal with them before they become larger and more “official”. Dealing with individual complaints effectively in the first place, can stop more negative press and reputational harm further down the line.

Regulatory Rights

The individual may, dependent on jurisdiction have recourse to the regulator, and may have the following rights: right to make a complaint to the regulator, right to a judicial remedy, right to be represented by legal or civil liberties organisations, and ultimately

right to compensation for damage or distress caused from their data misuse – whether that be accidental or deliberate.

- ☐ Ensure risks to individuals privacy are captured, and controls applied to minimise them.
- ☐ Ensure that processes are in place to provide copies of data to the individual on request, preferably on a self-service model.
- ☐ Ensure functionality is built into systems and processes to deal with rights requests effectively
- ☐ Ensure that complaints from individuals can be received and captured, and taken seriously by the IDSP.
- ☐ Ensure that procedures exist for ensuring that each individual's rights can be facilitated.
- ☐ Enable logging and tracking of requests from individuals, including the marking of data suspected to be inaccurate, or temporarily unable to be used.
- ☐ Ensure that procedures exists for interacting with regulators.

INTERNATIONAL TRANSFERS OF DATA

Increasingly legislation is trying to counteract or countermand the effect of global technologies. The advent of cloud-based computing and the internet has made data access effectively global, giving great utility to individuals who can gain access to data from any location at any time. However, the convenience of the cloud increases access to data from jurisdictions with variations in legal protections for individuals – as a result some privacy laws restrict movement of data across international boundaries where the rights and freedoms of individuals cannot be guaranteed.

Laws on national security may require the retention or localisation of data to a given jurisdiction. Some laws may also require that data to be held locally in certain jurisdictions for a given period, to enable access by law enforcement. These must be taken into consideration in determining storage and location of databases.

- ☐ Ensure that the full movement of personal data is recorded, so that international transfers can be identified.
- ☐ Respect laws that gate the use of data to a specific jurisdiction, or require local copies to be retained.
- ☐ Where legal justification needs to be held to ensure data transfer legitimacy, ensure records are kept.
- ☐ Aim to keep international transfers of personal data to a minimum.
- ☐ Choose providers that have valid international transfer mechanisms, and keep data in privacy protective jurisdictions where possible.

SECURITY

Information Security is a massive topic in its own right, and this code of practice will not seek to focus on all of the security controls that IDSP could employ. However, it cannot be denied the criticality of ensuring that high levels of security surround the issue and use of IDs, as it is then often used to gain access and authenticate to other services – when your ID is at risk, then access to all other forms of data also becomes compromised.

Attention should be paid to security management techniques and certifications, in particular the series of standards to provide complete management across the data lifecycle.

Risk assessment

Security is acknowledged as a business cost and a barrier to using data effectively. Therefore, a balance needs to be struck between security and usability, and equally a balance between the cost of the controls applied given an organisation's resources. The ideal security position is least spend for maximum return, understanding what controls to employ where based on a thorough understanding of the risks.

Methodologies exist (such as ISO 27005) to identify risks, quantify them and select mitigations, including a robust set of security controls. Obviously, security threats, technologies, laws, threats and vulnerabilities change over time, and so the risk assessment will need to be reviewed and updated at planned intervals.

Controls

Common ISO standards look at a wide security stance identifying a range of security controls, varying from preventive, detective, administrative to corrective control types. Controls should encompass the full gamut of security management areas, deployed in appropriate strength to counter and appropriate threat. For example in some areas a wooden door with a lock will suffice; in others, armed guards, surveillance and metal doors with biometric controls will be a more appropriate solution.

The standards group control different security domains, which include:

- ☐ Information security policies
- ☐ Organization of information security
- ☐ Human resources security
- ☐ Asset management
- ☐ Access control
- ☐ Cryptography
- ☐ Physical and environmental security
- ☐ IT Operational security
- ☐ IT Communications security
- ☐ Systems acquisition, development and maintenance
- ☐ Supplier relationships
- ☐ Information security incident management
- ☐ Information security aspects of business continuity management
- ☐ Legal and regulatory Compliance

Breach notifications

An organisation can never be 100% secure and therefore, inevitably, a breach may occur. The response required will vary by location; for example, some jurisdictions legally require notification to individuals and regulators. In any event, effective management of a security breach can determine the survivability of the organisation and reflects on the reputational harm that can result. It is important to react swiftly to introduce further controls to minimise harm to individuals; password resets, ID card cancellation or re-issue etc are key to ensure effective crisis management of any breach. The Information minimisation principles outlined above (such as anonymisation, or separation or minimisation) can certainly assist to reduce the impact of any breach).

Breach notifications should include:

- ☐ Nature of the breach, including the type and number of individuals affected, and the number of records affected.
- ☐ Timeline and circumstances of the breach, including the window wherein the breach may have occurred, or individuals data exposed.
- ☐ Name and contact details of individuals who can give further information, of all parties involved in the breach.
- ☐ Any consequences to individuals that may occur as a result.
- ☐ Any security measures and protections taken both before the breach, and after the breach, including those to mitigate any harmful effects.

Managing third parties

You cannot control what happens in third parties you have selected, but can take measures to manage the risks they pose, in their selection, contract and in the management and assurance obtained during their services.

In essence there are three key stages to managing third parties;

- **Pre contractual Due diligence** – ensuring that pre-contract, correct background checks and due diligence research has been carried out into the third party, including any necessary privacy by design or privacy impact assessments surrounding the processing by the third party.
- **Contract** – ensuring that the correct legal stipulations have been incorporated into contract to ensure the data is managed

correctly once the third party takes receipt. Contractual measures should include as a minimum:

- ☐ The mandate to process only for purposes and instructions received from the commissioning party, except where required by law.
 - ☐ Commitment of confidentiality, training of staff and staff confidentiality in contract.
 - ☐ Details of appropriate security measures required by the third party, and any certification and assurances required.
 - ☐ Requirements and procedure for any subcontracting of processing, including the requirement to pass on the same or more stringent requirements in contract to sub processors, and any permissions and assurances around changes.
 - ☐ Requirements surrounding the international transfer of data, including where applicable the requirement to ensure that adequate regards for individuals rights and freedoms are undertaken in any foreign territory.
 - ☐ Requirements to assist the facilitation of individuals rights.
 - ☐ Requirement to assist with any requests from regulators.
 - ☐ Requirement to document and make available all documentation to maintain compliance with the law, contract and this code of practice.
 - ☐ Details of how to terminate the contract, including whether data will be deleted or returned.
- **Post contractual management** – ensuring that the correct assurances have been received, and the contract is adhered to with appropriate measures, metrics, audits, certifications etc.

The level to which contractual compliance checks are carried out may vary according to the risk posed and importance of the third party supplier.

Data Access

Where there is authorised access to data there is a risk. Minimising access to data to smaller numbers of people, and subsequently reducing the data they have access to what is necessary for their role in a granular fashion can minimise risk exposure and the damage to the individual in the case of a breach.

- ☐ Ensure that the risks to individuals data from a security perspective are captured during the design process, are monitored effectively, and improved throughout operation.
- ☐ Employ technology-based security measures, but also ensure a culture of security, along with engaged management, staff training, physical and other security.
- ☐ Gain security certification, reviews and assurances in line with current best practices
- ☐ Limit access to data to the minimum necessary for carefully approved roles and entities.
- ☐ Ensure that security controls are established throughout the supply chain and that key suppliers are regularly reviewed for their compliance with security requirements.
- ☐ Ensure that any data breaches are notified through the supply chain, to the IDSP, and notified to regulators and individuals where required.

9. ADDITIONAL ISSUES FOR CONSIDERATION

MARRIAGE NAME CHANGES FORWARD AND BACK

Individuals may change their names over time, and life events such as marriage, divorce or legally-binding changes of name will cause records to change. Systems and processes created by IDSP should be designed with this in mind, and consideration should be given to whether an audit trail of previous names is retained. IDSP may of course require that individuals furnish them with appropriate legal records as proof of change.

METADATA TAGGING

Metadata is literally “data about data”. Often there is an assumption that metadata does not identify an individual, where in actuality it often does. There is often distinction drawn between “content” and “metadata”. For example in an email system, the content of the email is often considered of higher sensitivity than analysis of who is being emailed, when and how often. Data derived from the IDSP, such as the number of individuals in certain categories, or frequency and places of use of an ID, should be considered equally worthy of protection and as much part of the individual’s record as the data the individual has submitted themselves.

CULTURAL NORMS

In some areas there may be resistance or reluctance culturally to certain types of data collection, such as capturing images, or biometrics. Equally in some areas consent could be considered to be communally given, instead of from the individual, or males could be culturally considered to be able to consent on behalf of their partner. Whilst individual cultures should certainly be

respected, the rights of the individual should be held paramount, and the principles in this document applied to ensure equal treatment and respect for the individual.

DIGITAL RESILIENCE

Systems have been consistently designed in order that data is not lost, and certainly resilient systems include functionality such as cloud computing, back up data and multiple copies of information. Whilst data and systems should be resilient in the event of a disaster and to ensure the continuity of ID schemes, multiple copies of the data represent security risks – and each copy of the data should be carefully controlled and appropriate security applied – at least the same levels that are applied to the live data, as the data is of the same value. Indeed, backup copies can often face higher risks as they move, or are kept in more portable formats. Finally, there can be data integrity risks, where the data becomes unsynchronised, or is not up to date with the live copy, which should be carefully managed through its data lifecycle to deletion.

SEARCH FUNCTIONALITY

When giving individuals access to data, or making ID data searchable, consider carefully the use of the ability to search and export data, in that search functionality does not reveal data that users should not have had access to, or be able to consolidate and export batches of data without just cause. The use of privileged accounts especially should be logged, monitored and audited to make sure that system administrators with greater degrees of power are not able to export large batches of data without detection.

NAME SPELLINGS, SPOKEN LANGUAGE AND IDENTITY

Systems design can give rise to unconscious discriminatory effects or problems with identity management, where the format of a name or the language in which it is written in can be difficult to manage. Some languages may spell a male or female name differently, use different last name formats for married individuals, or contain special characters that the system was not designed to handle. For example, when looking at commercial biometric fingerprint readers to establish identity, it was found that the false positive rate was much higher than anticipated in Africa than in Europe. This was because the system design had been programmed with examples of European fingerprints, rather than fingerprints of samples locally obtained. When performing privacy by design activities, it is recommended that during the design phase, the scope and scale of the ID scheme is reviewed and any specific issues surrounding localised formats, languages, or cultural sensitivities are identified and managed appropriately.

INDEX OF WORDS

A

Access v–81, vi–81, 23–81,
43–81, 49–81, 52–81,
67–81, 68–81, 69–81

Accountability iv, 17, 70

Africa ii, iii, vi, vii, viii, 1, 2, 5, 6,
7, 8, 9, 28, 29, 55, 59, 75

African Union 2, 9, 28, 75, 76

age verification 33

anonymisation 22, 36, 37, 49

audit 19, 26, 27, 53, 65, 68, 69,
74

Automated Decision making
45

B

biometric 10, 37, 48, 55

C

certification 17, 26, 51, 52, 59,
69, 71

Collection Limitation v, 35

complaint 45, 71, 72

consent 30, 31, 33, 34, 38, 39,
43, 44, 53, 61, 62, 63, 66,
70

contract 26, 30, 31, 32, 50, 51,
62

controls 17, 22, 25, 26, 27, 46,
47, 48, 49, 52, 69

Convention 108 1, 29, 76, 77

crime 73

Cultural Norms vi, 53

D

data protection vii, 1, 2, 3, 5,
7, 8, 9, 11, 28, 29, 63, 69,
76, 77

data quality 40

E

ECOWAS 2, 29, 75, 76

Erasure v, 43

G

Government 8, 11, 15, 74

Government ID 15

I

ID cards 4, 15, 37

identity vii, 4, 5, 7, 10, 11, 12,
14, 15, 30, 33, 36, 39, 40,
41, 45, 55, 59, 61, 62, 63,
64, 65, 66, 67, 69, 73

ID Scheme iii, 12

IDSP iv, 15, 17, 18, 19, 20, 22,
33, 34, 39, 42, 43, 44, 45,
46, 47, 52

immigration 16

improvement 17, 19, 27

International transfer 23, 24

ISO 27701 17

L

legal basis 22, 29, 30, 31, 32, 33, 34, 35, 38, 39, 40, 43, 44

legal identity 4

Lifecycle iii, 12

M

Malabo Convention 28, 29, 59

metadata 21, 35, 53

Minimisation 22, 23, 36, 61, 65, 66

N

national ID 4, 9, 10, 11, 37

O

Objection v, 44

OECD 1, 8, 28, 75, 76

P

passport 30

personal data 8, 16, 17, 22, 26, 29, 30, 36, 47, 63, 66, 68, 69, 73, 74, 76

Portability v, 44, 67, 68, 69

privacy vii, 1, 2, 4, 5, 7, 8, 9, 10, 11, 17, 18, 19, 20, 21, 22, 24, 27, 28, 29, 32, 35, 36, 38, 39, 40, 43, 46, 47, 50, 55, 59, 61, 70, 74, 75

Privacy By Default iv

Privacy By Design iv

Privacy Laws vi, 2, 75

Privacy Management System 17

privacy principles 17, 19, 43

Pseudo anonymisation 36

Public interest 32

purpose 11, 30, 31, 33, 34, 35, 36, 37, 39, 42, 66, 72

Purpose Limitation v, 33

R

Records of Processing iv, 21

Rectification v, 44

Resilience vi, 54

Restriction v, 44

Rights ii, v, vii, 1, 4, 23, 42, 45, 73, 76

Risk Assessment vi

S

SADC 2, 29, 75

Security vi, 2, 23, 28, 42, 47, 48, 59, 70, 74

security breach 49

Special Category Data iv, 29

Storage Limitation, Retention and Deletion v, 41

supervisory authority 24, 39

U

United Nations 4, 7

UN 4, 7



APPENDIX – RESEARCH LIST

<https://www.gov.uk/government/consultations/draft-identity-assurance-principles/privacy-and-consumer-advisory-group-draft-identity-assurance-principles#the-nine-identity-assurance-principles>

<https://www.privacyinternational.org/feature/2274/identity-discrimination-and-challenge-id><https://www.gov.uk/guidance/identity-cards-and-new-identity-and-passport-service-suppliers>

https://en.wikipedia.org/wiki/ISO/IEC_7810

<https://www.iso.org/standard/31432.html>

<https://id2020.org/news/https/mediumcom/id2020/id2020-launches-technical-certification-mark-e6743d3f70fd>

https://docs.google.com/document/d/1LORhDq98xj4ieh5CuNP3XerK6umKRTPWMS8Ckz6_J8/edit

<https://ico.org.uk/for-organisations/guide-to-eidas/what-is-the-eidas-regulation/>

<https://www.brandsouthafrica.com/governance/government/how-to-apply-online-for-a-south-african-smart-id-card>

<https://www.theguardian.com/politics/idcards>

<https://www.simprints.com/impact>

<https://id2020.org/>

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386510

<https://www.iastoppers.com/week-1-making-aadhaar-mandatory-arguments-debate-week/>

Malabo Convention – Africa Union Convention on Cyber Security and Personal Data Protection

DPAS Newsletter - 2018 (1st Edition); Data Protection & Privacy Challenges in Africa by Teki Akuetteh Falconer

The World Bank's Identification for Development Strategic Framework (January 2016)

https://au.int/sites/default/files/treaties/29560-treaty-0048_-

african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

ID4D: 2018 report and their Principles on Digital ID.

McKinsey: useful report

ID4Africa: http://www.id4africa.com/2019/files/RADPA2019_Report_Blog_En.pdf

<https://www.courrierinternational.com/article/kenya-livrer-ses-donnees-personnelles-le-prix-payer-pour-lutter-contre-le-terrorisme>

https://edps.europa.eu/data-protection/our-work/edps-worldwide_fr#Regional%20&%20Int'l%20Networks

<http://documents.worldbank.org/>

[curated/en/835521468193502129/](http://documents.worldbank.org/curated/en/835521468193502129/)

[pdf/912490WP0FRENCO0Box385330B00PUBLIC0.pdf](http://documents.worldbank.org/curated/en/835521468193502129/pdf/912490WP0FRENCO0Box385330B00PUBLIC0.pdf)

<https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/>

<https://www.gemalto.com/france/gouv/tendance-des-cartes-electroniques-en-2016>

APPENDIX A – IDENTITY ASSURANCE PRINCIPLES

As an example - UK government Identity Assurance principles published at;

<https://www.gov.uk/government/consultations/draft-identity-assurance-principles/privacy-and-consumer-advisory-group-draft-identity-assurance-principles#the-nine-identity-assurance-principles>

1. The User Control Principle

Identity assurance activities can only take place if I consent or approve them.

An Identity Assurance Provider or Service Provider must ensure any collection, use or disclosure of IDA data in, or from, an Identity Assurance Service is approved by each particular Service-User who is connected with the IDA data.

Rationale/commentary

Identity Assurance Providers or Service Providers cannot use or disclose IDA data without the Service-User's knowledge and agreement (i.e. consent).

Service-Users must be able to control/choose whether or not to use or disclose their IDA data and whether or how they assert their identities.

Any exemption from the User Control Principle should be specified via the Exceptional Circumstances Principle.

The Data Minimisation Principle also applies to any collection, use and disclosure.

Legal commentary

The DPA requirement is that processing is either legitimised by consent of the data subject or is “necessary” for a contract with the data subject or is “necessary for a legal obligation or statutory functions of a public body etc (i.e. one of the schedule 2, paragraphs 1 to 6 of the DPA).

Consent takes the meaning in the Data Protection Directive (or any successor Regulation)

Also covers some “fair processing” requirements.

2. The Transparency Principle

Identity assurance can only take place in ways I understand and when I am fully informed.

Each Identity Assurance Provider or Service Provider must be able to justify to Service-Users why their IDA data are processed. Each Service-User, prior to using an Identity Assurance Provider or a Service Provider for the first time, must be provided with a clear description about the processing of IDA data in advance of any processing.

The information provided includes a clear explanation of why any specific information has to be provided by the Service-User (e.g. in order that a particular level of identity assurance can be obtained) and identifies any obligation on the part of the Service-User (e.g. in relation to the User’s role in securing his/her own identity information).

Any subsequent and significant change to the processing arrangements that have been previously described to a Service-User needs the prior consent or approval of that Service-User before it comes into effect.

Rationale/commentary

Organisations should engender trust by being open about all aspects of the processing of IDA data (Processing means

“collecting, using, disclosing, retaining, transmitting, copying, comparing, corroborating, aggregating, accessing” and anything else).

Such information does not need to be provided at every transaction, if the Service-User has been previously informed.

We expect that a public document explaining how these Principles have been applied to an Identity Assurance Service will be a valuable aid in meeting the objectives of this Principle (see also the Governance/Certification Principle below).

Where changes occur, any Provider would have to anticipate the fact that consent or approval might not be forthcoming.

Any exemption from the Transparency Principle should be specified via the Exceptional Circumstances Principle.

Legal commentary

First data protection principle requirement that the processing of personal data is fair.

3. The Multiplicity Principle

I can use and choose as many different identifiers or identity providers as I want to.

A Service-User is free to use any number of identifiers that each uniquely identifies the individual or business concerned.

A Service-User can use any of his identities established with an Identity Assurance Provider with any Service Provider.

A Service-User can choose any number of Identity Assurance Providers and where possible can choose between Service Providers in order to meet his or her diverse needs.

A Service-User shall not be obliged to use any Identity Assurance Provider or Service Provider not chosen by that Service-User; however, a Service Provider can require the Service-User to provide a specific level of Identity Assurance, appropriate to the Service-User's request to a Service Provider.

A Service-User can terminate, suspend or change Identity Assurance and where possible can choose between Service Providers at any time.

A Service Provider does not know the identity of the Identity Assurance Provider used by a Service-User to verify an identity in relation to a specific service.

Rationale/commentary

These first three need no explanation.

Obviously where there is a monopoly Service Provider (as is often the case with public sector services), then the Service-User does not have a choice of Service Provider. However, in general, there will be a number of Service Providers to choose from; this explains why the Principle uses "where possible".

Where Service Providers are a monopoly or near monopoly, they should not be able to require a particular Identity Assurance Provider to be used.

However, a Service Provider must be able to insist on a particular (and not unreasonable) level of identity assurance before delivering a service.

Any exemption from the Multiplicity Principle should be specified via the use of the Exceptional Circumstances Principle.

It should not be possible to link a Service-User's activities in different contexts.

4. The Data Minimsation Principle

My request or transaction only uses the minimum data that is necessary to meet my needs.

IDA data processed by an Identity Assurance Provider or a Service Provider to facilitate a request of a Service-User must be the minimum necessary in order to fulfil that request in a secure and auditable manner.

Note: it is useful to remind the reader that this principle has a wide reach because of the definitions of IDA data and Processing:

- “IDA data includes “Personal data”, “Audit data”, “Attribute data”, “Identity data”, “Relationship data”; “Transactional data” and other “General data”.
- “Processing” in the context of IDA data means “collecting, using, disclosing, retaining, transmitting, copying, comparing, corroborating, aggregating, accessing” etc.

Rationale/commentary

So for the absence of doubt, any aggregation, correlation or corroboration of IDA data from diverse Identity Assurance Providers or Service Providers are subject to all the Identity Assurance Principles.

All IDA data processed has to be the minimum necessary in the context of service delivery or identity verification. Note that a Service User can, for his own convenience, request a Provider to hold information beyond the minimum necessary. Subject to any audit or legal requirement, the Minimisation Principle requires any aggregation, correlation or corroboration to be of a transient nature.

Data minimisation is a very important design criterion; we expect compliance with this Principle will be an essential component of any Identity Assurance Service.

Any decision that requires a risk assessment of the Service-User will need the correlation of data from possibly a number of sources will also be subject to the Data Minimisation Principle. Note that the User Control or Transparency Principle should ensure the Service-User can provide informed consent/approval. There should be no centralisation of IDA data.

Any exemption from the Data Minimisation Principle should be specified via the Exceptional Circumstances Principle.

Legal commentary

Third and Fifth Data Protection Principles (“Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed” and “kept no longer than is necessary”).

The Data Protection Regulation currently being discussed by the European Commission and Member States aims to further strengthen the personal data minimisation requirements beyond those set in the Third Data Protection Principle of the 1998 Act. This is supported by Data Protection by Design objectives that also appear in the Regulation.

5. The Data Quality Principle

I choose when to update my records.

Service-Users should be able to update their own personal data, at a time at their choosing, free of charge and in a simple and easy manner.

Identity Assurance Providers and Service Providers must take account of the appropriate level of identity assurance required before allowing any updating of personal data.

Rationale/commentary

Unnecessary retention and excessive data collection would breach the Data Minimisation Principle.

If a Service User fails to keep his information up to date, then his transactions could fail; this we believe is the incentive for Users to keep information up to date.

Any legal obligation that requires, for example, an individual to notify a public authority of a change of circumstances is unaffected; a Service-User can choose to use an Identity Assurance System, at any chosen time, to update their own records subject to any identity assurance requirement prior to accepting an update.

As failed transactions (e.g. by virtue of a data mismatch) are likely to be alerted to Service-Users, this affords a possibility of designing procedures that offer Service-Users the opportunity to update their own details immediately – again subject to any identity assurance requirement prior to accepting any update.

The Identity Assurance/Service Provider has to be able to decide the level of identity assurance before accepting a change to a Service User's data.

Any exemption from the Data Quality Principle should be specified via the Exceptional Circumstances Principle.

Legal commentary

Accuracy requirements of DPA (4th Principle).

6. The Service-User Access and Portability Principle

I have to be provided with copies of all of my data on request; I can move/remove my data whenever I want.

Each Identity Assurance Provider or Service Provider must allow, promptly, on request and free of charge, each Service-User access to any IDA data that relates to that Service-User.

It shall be unlawful to make it a condition of doing anything in relation to a Service-User to request or require that Service-User to request IDA data.

The Service-User shall have the right to require an Identity Assurance Provider to transmit his personal data, to a second Identity Assurance Provider in a standard electronic format, free of charge and without impediment or delay.

The Service-User's right to data portability shall also apply between Service Providers.

Rationale/commentary

For the absence of doubt, such access includes access to logs of Service-User activity, disclosure logs of any Service-User data, and any audit data relating to that Service-User's activity but excludes any anonymised data that can no longer be linked or associated with a particular Service-User.

The prohibition is needed as there is a practice in the UK of requiring data subjects to use their subject access rights to criminal records and medical records and show the product of their access request to an employer or insurer. The prohibition stops unscrupulous use of the access right. The text is based on the prohibition in the ID Card Act 2005.

This is the right to data portability.

Any exemption from the Service-User Access and Portability Principle should be specified via the Exceptional Circumstances Principle.

Legal commentary

Subject access under the DPA.

Privacy by Design (under the heading Data Protection by Design) should include a user access functionality; free Subject Access is part of the European Union's Data Protection Regulation under discussion.

Stopping Enforced Subject Access is very important.

(Data Portability forms part of the European Union's Data Protection Regulation under discussion).

7. The Governance/Certification Principle

I can have confidence in any Identity Assurance System because all the participants have to be accredited.

As a baseline control, all Identity Assurance Providers and Service Providers shall be certified.

There shall be a certification procedure subject to an effective independent audit regime which ensures that all relevant, recognised identity assurance and technical standards, data protection or other legal requirements are maintained by Identity Assurance Providers and Service Providers.

In the context of personal data, certification procedures include the use of Privacy Impact Assessments and Privacy by Design concepts.

All Identity Assurance Providers and Service Providers shall take all reasonable steps to ensure that a Third Party cannot capture IDA data that confirms (or infers) the existence of relationship between any Participants.

Certification can be revoked if there is significant non-compliance with any Identity Assurance Principle. The architecture of an Identity Assurance Service must be based on open standards.

Rationale/commentary

This Principle mandates the use of all relevant standards as the baseline for all information assurance/security/integrity controls used.

We expect that this Principle will require the production of a document that describes how the design of the Identity Assurance Service has been informed by the application of the Identity Assurance Principles to the design (See also the Transparency Principle above).

The “reasonable steps” tries to ensure that web-based services cannot capture details of a relationship between a Service User and any Identity Assurance Provider or Service Provider (for example through the use of webcrawlers or webspiders).

(Note: this is why relationship data includes in its definition relevant cookies and programs that collect such data.)

Any exemption can be specified via use of the Exceptional Circumstances Principle, but we don’t expect many (or indeed any!).

Legal commentary

The Accountability Principle in the Data Protection Regulation (currently under discussion in Europe); the current obligations in the Seventh Data Protection Principle (or HMG Security Framework or ISO27000) are expected to form part of the Certification process.

Privacy Impact Assessments and Privacy by Design concepts will be legal obligation if the European Commission’s Data Protection Regulation becomes law (see under the heading Data Protection by Design and Data Protection Impact Assessments).

Consideration needs to be given as to whether it should be made unlawful for such details to be captured (even overriding any User’s explicit consent). We are very concerned that many Users do not know what permissions they have given nor do they read privacy policies of organisations based outside the EEA. There is a need to take away the defence of a Third Party that it has

the permission of the User to capture details from an Identity Assurance Service.

8. The Problem Resolution Principle

If there is a problem I know there is an independent arbiter who can find a solution.

A Service-User, who after a reasonable time, cannot or is unable to resolve a complaint or problem directly with an Identity Assurance Provider or Service Provider can call upon an independent Identity Ombudsman to seek independent resolution of the issue.

As part of the certification process, Identity Assurance Providers and Services Providers are obliged to co-operate with the Identity Ombudsman and accept his impartial determination and to ensure that contractual arrangements:

- reinforce the application of the Identity Assurance Principles
- contain a reference to the Identity Ombudsman as a mechanism for problem resolution

The Identity Ombudsman can resolve the same or similar complaints affecting a group of Service-Users.

The Identity Ombudsman can co-operate with other Regulators in order to resolve problems and can raise relevant issues of importance concerning an Identity Assurance Service.

An adjudication/recommendation of the Identity Ombudsman shall be published.

There can be more than one Identity Ombudsman.

The Identity Ombudsman can recommend changes to standards or certification procedures or that an Identity Assurance Provider or Service Provider should lose their certification.

Rationale/commentary

The central problem is that many different Regulators (e.g. Information Commissioner; FSA, OFCOM) could be involved and that an individual has to be able to complain to a central point of contact in order to resolve an issue.

Without an Ombudsman/Advocate, there is a risk that the Service User will be passed from pillar to post.

One assumes, however, that a Service-User will resolve a complaint in the usual way. However, it is possible that complaints will not be resolved satisfactorily.

We expect that any determination made by an Identity Ombudsman can be appealed to the Courts by any party to the dispute.

Any exemption from the Problem Resolution Principle can be specified via use of the Exceptional Circumstances Principle (but we can't see the need of any exemption as explained as follows). Take an extreme example, and suppose there was an exemption needed for say "national security", then the Regulator who has the responsibility for the national security function could be designated as the "ombudsman" for that purpose. This would maintain the integrity of this Principle and the secrecy required of the national security function.

9. The Exceptional Circumstances Principle

Any exception has to be approved by Parliament and is subject to independent scrutiny.

Any exemption from the application of any of the above Principles to IDA data shall only be lawful if it is specified in a statutory framework that legitimises all Identity Assurance Services, or an Identity Assurance Service in the context of a specific service.

Any exemption from the application of any of the above Principles that relates to the processing of personal data must also be necessary and justifiable in terms of one of the criteria in Article 8(2) of the European Convention of Human Rights: namely in the interests of national security; public safety or the economic well-being of the country; for the prevention of disorder or crime; for the protection of health or morals, or for the protection of the rights and freedoms of others.

Any subsequent processing of personal data by any Third Party who has obtained such data in exceptional circumstances (as identified by Article 8(2) above) must be the minimum necessary to achieve that (or another) exceptional circumstance.

Any exceptional circumstance involving the processing of personal data must be subject to a Privacy Impact Assessment by all relevant “data controllers” (where “data controller” takes its meaning from the Data Protection Act).

Any exemption from the application of any of the above Principles in relation to IDA data shall remain subject to The Problem Resolution Principle.

Rationale/commentary

There are a myriad of data sharing laws each with different standards and rules. To engender trust in identity assurance and to improve Parliamentary scrutiny, it is proposed that ONLY statutory gateways created by any legislation needed to establish the programme are valid. There might be a phasing in period (as discussed in the workshop).

The special interests identified in Article 8(2) are expressly put into this Principle. However, the linkage to individual human rights means that the link can only relate to personal data (i.e. an identifiable living individual). This is why a definition of “personal data” is needed.

This allows for limited onward data sharing, so long as it is consistent with Article 8 of the HRA. There is a real issue as to whether the current level of privacy protection is adequate for some public bodies (e.g. is the protection in RIPA adequate? is the Regulatory regime for the Security Service, GCHQ or the Police OK?).

Our construction avoids the opening up of what would be an everlasting debate; however, the last paragraph of this Principle is the necessary “quid pro quo” for this position. (See comments at the bottom of Principle 8 re Governance on national security.)

Legal commentary

The Privacy and Consumer Advisory Group to the Government’s IDA Programme recommends that legislation is enacted to implement the Government’s Identity Assurance Plans. Any such legislation would be the natural vehicle to describe all aspects falling under the “Exceptional Circumstances Principle”.

It is expected that any exemption will be limited, and expressed in terms of particular subsets of IDA data (e.g. “personal data”, “audit data”, “relationship data”) necessary for the application of any exemption.

The European Commission’s Data Protection Regulation calls for mandatory Data Protection Impact Assessments (i.e. Privacy Impact Assessments).

APPENDIX B – PRIVACY LAWS ACROSS AFRICA

(Credit: Greenleaf, Graham, Countries with Data Privacy Laws – by Year 1973-2019 (June, 2019). Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386510)

Key Law column = name of current key law (Earlier key laws may have had different names)

From column Year = year of original data privacy law enacted, for either private or public sector; might not be year of current law

Latest column Year = year of last significant version of law (amendment or replacement) known; 'NYIF' = not yet in force, where bringing into force is delayed more than two years; 'B(201x)' = current official reform Bill, not yet enacted, and year.

Member column: listing means country is a member of regional grouping relevant to data privacy (plus '(A)' for Associate members)

OECD = Organisation for Economic Cooperation and Development;

AU = African Union;

ECOWAS= Economic Community of West African States;

EAC= East African Community;

SADC= Southern African Development Community;

ECCAS= Economic Community of Central African States;

CEMAC = Communauté économique et monétaire de l'Afrique centrale

International Agreements column = covers the following agreements between countries, each of which involves legal obligations (for APEC Framework and OECD Guidelines, see Member column, as all Members have the same non-binding commitments). No entry means country has taken no action

- i. European Union General Data Protection Regulation = GDPR, plus one of M = country is an EU member state; AQ = country's protection of personal data has been held 'adequate' by the EU under GDPR or 1995 Directive; EEA = country is a member of the European Economic Area; OCT = Overseas Countries and Territories status; EUT = part of territory of an EU country.
- ii. Convention 108 = CoE108 (means has ratified Treaty 108) plus one of: RP = has ratified Additional Protocol; SP = has signed but not ratified Additional Protocol (Treaty 181); RC* = UK has ratified CoE108 on behalf of sub-jurisdiction; (AC) = non-European state has acceded to CoE108; (IA) = non-European state invited to accede to CoE108;
- iii. Convention 108+(Treaty 223) = CoE 108+ plus either (S) = signed or (R) = ratified.
- iv. (iv) African Union Convention = AUConv plus either (S) = signed or (R) = ratified.
- v. ECOWAS Act = country is required to comply with the additional data protection Act to the ECOWAS Treaty, 2010.
- vi. APEC-CBPRs (Cross-Border Privacy Rules system) = APEC-CBPRs, plus either (S) = has agreed to participate (but no AA appointed), or (AA) = is participating (AA appointed).

- vii. UN International Convention on Civil & Political Rights= ICCPR
= ratified ICCPR (unless (S) = signed); +OP= ratified 1st
- viii. Optional Protocol; [Not-UN] = not UN member, cannot ratify

Authority column: DPAs are named = 'Not yet appointed' if not; or 'None' = no specialised data protection authority.

DPA Associations column: inclusion means 'DPA is a member of' the named association of DPAs/PEAs; except (O) = Observer status only:

ICDPPC = International Conference of Data Protection and Privacy Commissioners(except'(O)' for Observers status for at least 3 years); GPEN= Global Privacy Enforcement Network; AFAPDP= Association of Francophone Data Protection Authorities; RedIPD = RED Iberoamericana de Preteccion de Datos;; CTN= Common Thread Network (anglophone Commonwealth of Nations); RAPDP= Réseau Africain sur la Protection des Données Personnelles (African Personal Data Protection Network); GCBCEA= Global Cross Border Enforcement Cooperation Arrangement.; GPEN-A= GPEN Alertmember ; RAPDP= Réseau Africain sur la Protection des Données Personnelles (African Personal Data Protection Network); RNDPAEPC= Regional Network of Data Protection Authorities in Eastern Partnership Countries member; CoE108CC= Convention 108 Consultative Committee member; Except (O) = Observer status only

Country	Key Law	From	Latest	Membership	Sector		Authority	DPA Assocs
Algeria	Act on the Protection of Personal Data	1999	2014	AU	Both	ICCPR + OP	Not yet appointed (Autorité Nationale de Protection des Données à Caractère Personnel)	-
Angola	Lei da Protecção de Dados Pessoais	2011	2011	AUSADC, ECCAS	Both	ICCPR+OP	Agência da Protecção de Dados	-
Benin	Code du Numérique	2009	2017	AU/ECOWAS	Both	ICCPR+OP; AUConv(S)	National Commission for Technology and Freedoms (Commission nationale de l'informatique et des libertés)	CDPPC; AFAPDP; RAPDP
Burkina Faso	Loi Portant Protection des Données à Caractère Personnel	2004	2004	AU/ECOWAS	Both	CCPR+OP; AU Conv(S); ECOWAS Act; CoE108(A)	ata Processing and Liberties Commission	ICDPPC; AFAPDP; RAPDP; CoE108CC (O)
Cape Verde	Regime Jurídico Geral de Protecção de Dados Pessoais a Pessoas Singulares	2001	2013	AU/ECOWAS	Both	ICCPR+OP; CoE108(RP); ECOWAS Act	National Commission of Data Protection	ICDPPC; RAPDP; RedIPD; AFDAIP; CoE108CC
Chad	Law No. 007/PR / 2015 on the Protection of Personal Data	2015	2015	AU; ECCAS	Both	ICCPR+OP; AUConv(S); ECOWAS Act	Not yet appointed(National Agency for Information Security and Electronic Certification)	-
Cote d'Ivoire Africa	Loi relative à la protection des données à caractère personnel du 19 juin 2013	2013	2013	AU; ECOWAS	Both	ICCPR+OP; AUConv(S)	Telecommunications / ICT Regulatory Body of Côte d'Ivoire - Autorité de régulation des télécommunications et des TIC (ARTCI)	ICDPPC; AFAPDP; RAPDP

Country	Key Law	From	Latest	Membership	Sector	International Agreements	Authority	DPA Assocs
Equatorial Guinea	Ley de Protección de Datos Personales (Law 1/2016)	2016	2016	AU; ECCAS; CEMAC	Both	ICCPR+OP;	Not yet appointed (Organo Rector de Protección de Datos Personales)	-
Gabon	Law related to personal data	2011	2011	AU; ECCAS; CEMAC	Both	ICCPR;	Commissariat à la protection des données personnelles	AFAPDP; RAPDP; CoE108CC (O)
Ghana	Data Protection Act	2012	2012	AU; ECOWAS	Both	ICCPR+OP; AU Conv(S); ECOWAS Act	Data Protection Commission	ICDPPC; CTN/RAPDP; GPEN; CoE108CC(O)
Guinea (Conakry)	Loi L/2016 /037/AN relative à la cyber - sécurité et la protection des données à caractère personnel	2016	2016	AU; ECOWAS	Both	ICCPR+OP; AU Conv(R); ECOWAS Act	Not yet appointed (National Data Protection Authority)	-
Lesotho	Data Protection Act	2011	2011	AU; SADC	Both	ICCPR+OP;	Data Protection Commission	-
Madagascar	Loi N° 2014-038 Sur la protection des données à caractère personnel	2015	2015	AU/SADC	Both	ICCPR+OP	Not yet appointed (Commission Malagasy sur l'informatique et les Libertés (CMIL)	-
Malawi	Electronic Transactions And Cyber Security Act, 2016	2016	2016	AU; SADC	Both	ICCPR+OP	Malawi Communications Regulatory Authority	-

Country	Key Law	From	Latest	Membership	Sector	International Agreements	Authority	DPA Assocs
Mali	Loi no 2013/015 du 21 mai 2013 portant protection des données à caractère personnel	2013	2013	AU; ECOWAS	Both	ICCPR+OP; ECOWAS Act; AUCov(S)	Personal Data Protection Authority (Autorité de Protection de Données à Caractère Personnel)	ICDPCC; RAPDP; AFAPDP
Mauritania	Loi 2017 - 020 sur la protection des données à caractère personnel	2016	2016	AU; ECOWAS (A)	Both	ICCPR; AU Conv(S); ECOWAS Act	Not yet established (Autorité de protection des données)	-
Mauritius	Data Protection Act	2004	2017	AU; SADC	Both	ICCPR+OP; CoE108(RP); AU Conv(R)	Data Protection Office of Mauritius (Commissariat à la protection des données personnelles)	ICDPCC; AFAPDP; GPEN; CTN; RAPDP; CoE108CC
Morocco	Loi relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel	2009	2009	AU	Both	ICCPR; CoE108(A)	National Commission for the Control and the Protection of Personal Data (CNDP) (Commission nationale de contrôle et de protection des données personnelles)	ICDPCC; AFAPDP; RAPDP; GPEN; CoE108CC (O)
Niger	Loi 2017- 28 relative à la protection des données à caractère personnel	2017	2017	AU; ECOWAS	Both	ICCPR+OP; AUCov(S) ECOWAS Act	Not yet appointed (National Data Protection Authority)	-
São Tomé and Príncipe	Data Protection Law	2016	2016	AU; ECCAS	Both	CoE108 (IA); AUCov(S) CCPR+OP	Agência Nacional de Protecção de Dados Pessoais	-

Country	Key Law	From	Latest	Membership	Sector	International Agreements	Authority	DPA Assocs
Senegal	Loi sur la Protection des données à Caractère Personnel	2008	2008	AU; ECOWAS	Both	ICCPR+OP; CoE108(RP); ECOWAS Act; AUCov(R)	Commission of Personal Data Protection, CDP (La Commission de Protection de Données Personnelles)	ICDPPC; AFAPDP; RAPDP; CoE108CC
Seychelles	Data Protection Act	2004	2004 NVIF	AU; SADC	Both	ICCPR+OP;	Not yet appointed (Data Commissioner)	CTN(O)
South Africa	Protection of Personal Information Act	2013	2013 NVIF	AU; SADC	Both	ICCPR+OP;	Information Regulator	ICDPPC; RAPDP; CTN
Tunisia	Loi portant sur la protection des données à caractère personnel	2004	2004 B(2018)	AU	Both	ICCPR+OP; CoE108(RP)	National Personal Data Authority	ICDPPC; AFAPDP; RAPDP; CoE108CC
Zimbabwe	Access to Information and Protection of Privacy Act	2002	2002 B(2018)	AU; SADC	Public	ICCPR;	Media Commission	-

NO CURRENT LAWS: Botswana, Burundi, Cameroon, Central African Republic, Democratic Republic of the Congo, Djibouti, Eritrea, Gambia, Liberia, Libya, Mayotte, Melilla, Mozambique, Namibia, Reunion, Rwanda, Somalia, Sudan, Togo, Uganda, Western Sahara –

CURRENT LAWS PROPOSED: Cormoros, Egypt, Ethiopia, Nigeria, Kenya, Tanzania, Zambia,

The Code of Practice (COP) facilitates the adoption and implementation of good practices that ensure adequate protection and guarantee of the right to privacy of subjects of digital identity schemes in Africa. It is a guide to the adoption and implementation of standards and/or processes that assure good data protection practices for the development and use of digital identity schemes. It is a generic tool developed based on knowledge and appreciation of both the African landscape and international best practices. The Code of Practice is a useful guide/manual to policy makers, regulators, digital ID and addressing developers and implementors (both government and private sector) in Africa. It is a 'do-it-yourself' guide towards achieving good IDs by applying a principle-based approach to privacy and data protection to the development and use of digital identity schemes for both commercial and governmental use. It serves as a "toolkit workbook" that gives organisations a structured approach to assessing the risks of harm to digital identity and provides practical steps to reduce those risks. It covers at the data protection landscape in Africa, organisational accountability, data protection/privacy principles and other issues for consideration on digital identity schemes and data protection/privacy in Africa.

ISBN: 978-9988-54-744-8



9 789988 547448