

International recommendations for the use of personal data

Yaël Hirsch

5 November 2015



Content

African regulatory landscape

- Overview
- Key expectations
- Similarities with European data protection regulation

General Data Protection Principles

- Definitions
- Key Principles
- Health Data

Key recommendations

- Comply with the Health regulation
- Formalities prior to implementing a data processing
- Transfer of data

African regulatory landscape

African regulatory landscape

African organizations

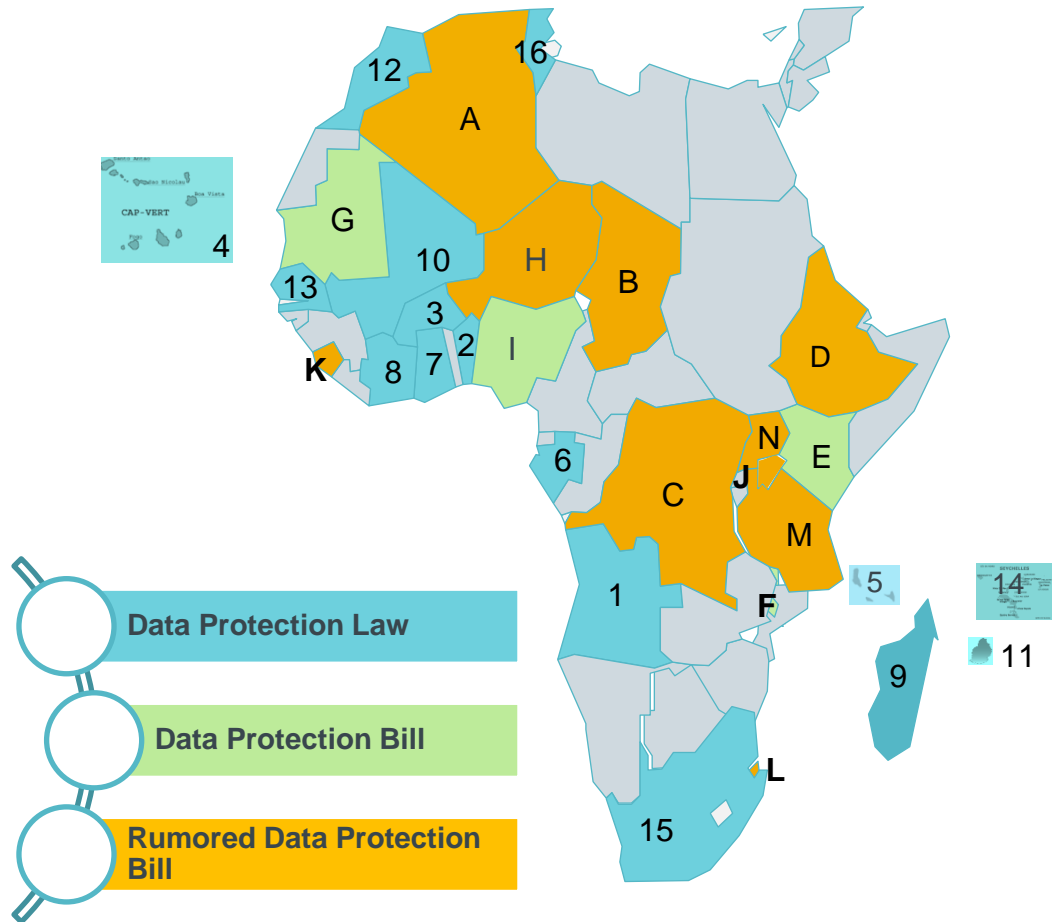
- African Union
- ECOWAS

African countries having adopted a DP regulation

- | | |
|-----------------|-------------------------------|
| 1. Angola | 10. Mali |
| 2. Benin | 11. Mauritius |
| 3. Burkina Faso | 12. Morocco |
| 4. Cape Verde | 13. Senegal |
| 5. Comoros | 14. Seychelles (Not in force) |
| 6. Gabon | 15. South Africa |
| 7. Ghana | 16. Tunisia |
| 8. Ivory Coast | |
| 9. Madagascar | |

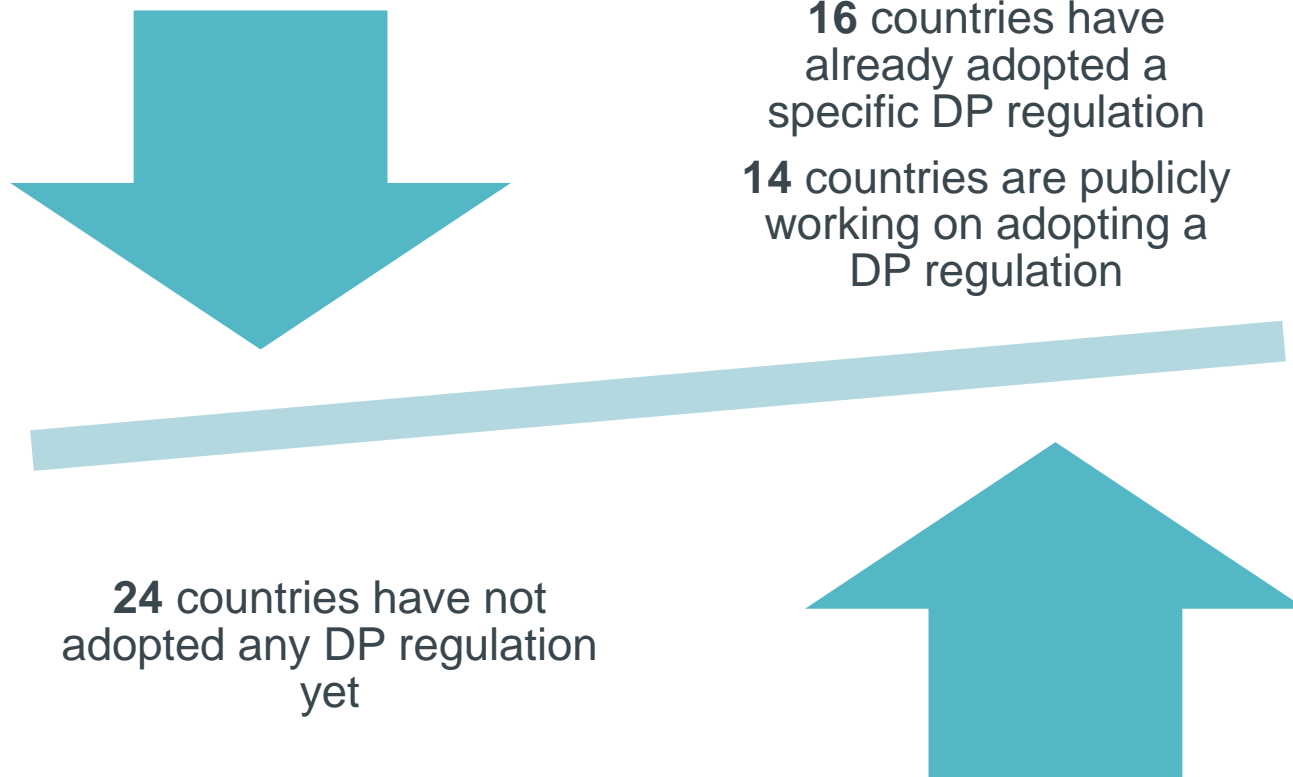
DP Bills

- | | |
|---------------|-----------------|
| A. Algeria | I. Nigeria |
| B. Chad | J. Rwanda |
| C. DRC | K. Sierra Leone |
| D. Ethiopia | L. Swaziland |
| E. Kenya | M. Tanzania |
| F. Malawi | N. Uganda |
| G. Mauritania | |
| H. Niger | |



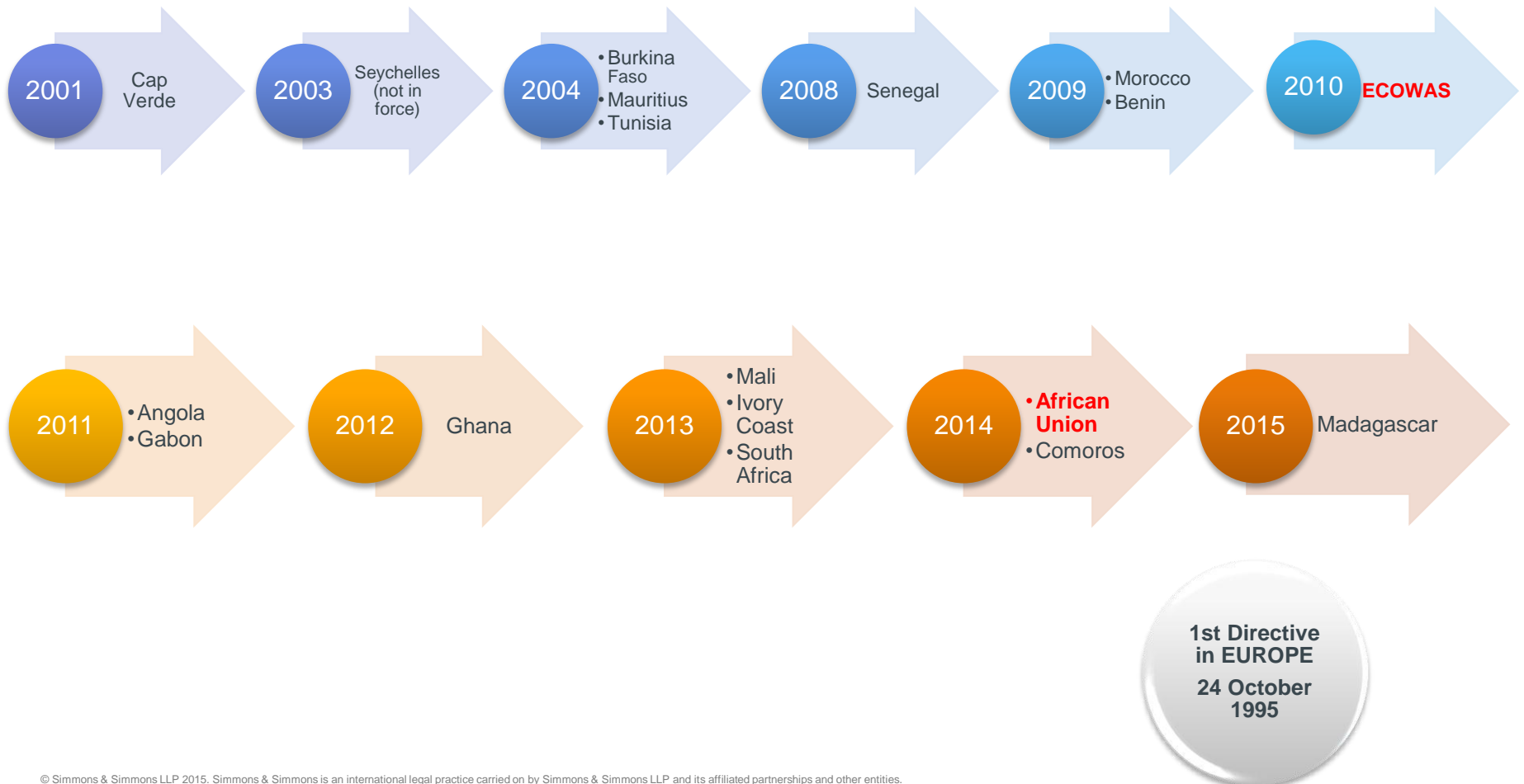
African regulatory landscape

Wide continental development



African regulatory landscape

Laws adoption dates



African regulatory landscape

27 June 2014 - Adoption of African Union Convention on Cyber Security and Personal Data Protection

- **Major 1st step:** for the first time, at a continent scale, States agreed on a legal framework to regulate and promote efficiently ICT activities (e-transactions, PD protection, Cyber security and cybercrime)
- The Convention **sets forth the legal and institutional framework for the protection of personal data** to be implemented by the signatory States
- **National legislations shall be adopted or at least amended** to comply with the principles set forth in the Convention
- The Convention is however **not a ready-to-use legal instrument** and States members shall in particular detail the appropriate provisions (including technical aspects) on the basis of the principles agreed in the Convention
- The transposition process of the Convention should give **much leeway to the States** with respect to its implementation, interpretation and enforcement especially since States are allowed to formulate reserves preventing the achievement of a total harmonization
- The Convention **shall enter into force 30 days** after the fifteenth ratification is received. To this date, no Member State has ratified the Convention

African regulatory landscape

Trends in data protection regulation in Africa

- Along with the **rapid growth of the digital economy in Africa**, the need for **adequate regulation** of the ICT sector is getting stronger.
- Several countries have adopted new data protection laws.
- **Not one legislation but a multitude of legislations** rendering pan-African project difficult to implement
- **Great Influence of EU regulation** on data protection laws in the continent including the new monitoring mechanisms
 - Recently, Madagascar has incorporated in its legislation a **data privacy officer**: designed by the data controller and it exonerates from prior notification formalities to the authority
 - **Open data**: *Data or content is open if anyone is free to use, re-use or redistribute it, subject at most to measures that preserve provenance and openness* (World Bank)
 - **Open data** initiatives:
 - Morocco administration's open data webpage: <http://data.gov.ma/fr>
 - Kenya public government's open data webpage <https://opendata.go.ke/>
- **Ongoing challenges**: many countries have yet to set up and fund their national protection authority or adopt a comprehensive regulation especially to control the uprising of various ICT services such as IoT, mobile banking, Big data.

General Data Protection Principles

Definitions

What's a personal data?



Personal data means any information

- relating to an identified or identifiable natural person
- by which this person can be identified, directly or indirectly
- in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Health data means all information relating to the physical or mental state of the data subject, including the aforementioned genetic data.

Definitions

Who is the Data controller and a processor?

- **Data Processing**: Broad definition - operation or set of operations which is performed upon personal data
- **Data controller**: any person who **decides to collect and process** personal data and **determines the purposes**
 - a medical practitioner is usually the controller of his patients' data
 - a laboratory or public organization which orders the research are the controllers for the data processed during the trials
- **Data processor**: third party that implements the processing – subcontractor
 - a practitioner which implement de trials

Both should respect data protection regulations

Accountability of the data controller

Key Principles

General Data Protection Principles

- Collecting exclusively carried out for **lawful, specific and explicit purposes**
 - Determining the research objectives and justifying the data needed to fulfill these objectives
 - Verifying if the objective of the research is lawful
- PD collected must be **appropriate, relevant and non-excessive for the purpose** for which they are collected
 - Limiting the collection of personal data
- Setting **reasonable time limits on retention** of personal data
 - Processed PD shall not be kept longer than what is necessary to accomplish the determined purpose

Key Principles

General Data Protection Principles

- Data controller must take all necessary precautions to insure the **security and confidentiality** of the PD
 - Safeguarding personal data (cryptology, firewall, physical security)
 - Controlling access and disclosure of personal data
- Obtaining the **informed consent** of the prospective research participants
 - Determining if consent from individuals is required
 - Managing and documenting consent
 - Informing the participant about their rights and the research
- Complying with preliminary formalities
 - Authorization or declaration
 - Other specific regulation

Key Principles

Administrative and penal sanctions e.g South Africa

- **Civil remedies:** A court hearing proceedings may award **compensation to data subjects** whether there is intent or negligence from the data controller

- **Administrative sanctions**
 - The Regulator may issue an **infringement notice** if a person is alleged to have committed in offence with respect to this Act
 - The alleged infringer may chose to be tried by a Court instead of the Regulator
 - An **administrative penalty** in an amount **not exceeding Rand 10 million (approximately 765,800 euros)** may be imposed as an alternative to a criminal sanction
 - The **Minister may**, from time to time and after consultation with the Regulator, by notice in the Gazette, **adjust the amount maximum of the** fine in accordance with the average consumer price index

- **Criminal penalties** can apply for offences including:
 - **Failure to notify a processing requiring a prior authorization** is punishable by a fine (amount not specified) and/or an imprisonment for a period **not exceeding 12 month**
 - The **unlawful obstruction, interference or influence of the Regulator** is punishable by a fine and/or an imprisonment for a period **not exceeding 10 years**
 - **Breach of confidentiality** is punishable by a fine and/or an imprisonment for a period **not exceeding 12 month**
 - Failure to comply **with enforcement or information notices** is punishable by a fine and/or an imprisonment for a per period **not exceeding 10 years**

Health Data

Main Principles

- **Concept of sensitive data:** unless otherwise provided the processing of personal data related, directly or indirectly, to health is forbidden e.g Tunisia, Benin

- **Exceptions:**
 - The data subject has given his/her written consent
 - Research purpose

- **Formalities**
 - Authorization requests: Tunisia, Morocco, Senegal, Angola, Ivory Coast, South Africa
 - Other: e.g Gabon
 - **Advisory Committee** instituted by the Minister issue an opinion on the methodology of the research with respect to the law and the necessity to process personal data (one month to issue its opinion)
 - Authorization requested to the data protection authority
 - Possibility of simplified request for usual processing.

Key recommendations

Key recommendations

Comply with health regulation

- Doctor-Patient confidentiality
- Obligation of security of the data
- Formalities of the research
- Certified hosting service provider

Obtain an informed consent

- Detailed information regarding the research (purpose, scope, steps)
- Detailed information on the processing
- Rights: access, rectification and opposition
- If there are transfer of data, to whom and where

Follow Data Protection Formalities

- Depending on the purpose of the processing
- Depending on the type of data
- Research protocols, if any (e.g. in France, MR001)
- Security protocol

Transfer of data

- Adequate level of protection of the privacy, freedoms and fundamental rights of persons whose data are being or are likely to be processed
- Limited exceptions to the interdiction of international transfers: e.g. Transfer contracts; BCR; Safe Harbour (illicit towards to US following ECJ decision in October 2015)
- Anonymization of the data
- Information of the participant

International coverage



Amsterdam
Brussels
Bristol
Düsseldorf
Frankfurt
Funchal *
Lisbon *
London
Luxembourg
Madrid
Milan
Munich
Paris
Rome



Abu Dhabi
Doha
Dubai
Jeddah **
Riyadh **



Beijing
Hong Kong
Shanghai
Singapore
Tokyo

**Sociedade Rebelo de Sousa in association with Simmons & Simmons LLP*

***Hammad & Al-Mehdar in alliance with Simmons & Simmons*

Yaël Hirsch

Yael.hirsch@simmons-simmons.com

simmons-simmons.com
elexica.com