Emerging Data Protection regulations in Africa

Christophe Fichet

19 May 2015
Development of data protection laws in Africa

Key expectations over the next year
Data Protection landscape

- African organizations
  - African Union
  - ECOWAS

- African countries having adopted a DP regulation
  1. Angola
  2. Benin
  3. Burkina Faso
  4. Cape Verde
  5. Comoros
  6. Gabon
  7. Ghana
  8. Ivory Coast
  9. Madagascar
  10. Mali
  11. Mauritius
  12. Morocco
  13. Senegal
  14. Seychelles
  15. South Africa
  16. Tunisia

- DP Bills (and rumoured bills)
  A. Algeria
  B. Chad
  C. DRC
  D. Ethiopia
  E. Kenya
  F. Malawi
  G. Mauritania
  H. Niger
  I. Nigeria
  J. Rwanda
  K. Sierra Leone
  L. Swaziland
  M. Tanzania
  N. Uganda
  O. South Africa
  P. Cameroon
  Q. Ethiopia
  R. Kenya
  S. Malawi
  T. Mauritania
  U. Nigeria
  V. Senegal
  W. Tanzania
  X. Tunisia
  Y. Algeria
  Z. Chad
  AA. DRC
  BB. Ethiopia
  CC. Kenya
  DD. Malawi
  EE. Mauritania
  FF. Niger
  GG. Nigeria
  HH. Rwanda
  II. Sierra Leone
  JJ. Swaziland
  KK. Tanzania
  LL. Uganda
  MM. South Africa
  NN. Cameroon
  OO. Ethiopia
  PP. Kenya
  QQ. Malawi
  RR. Mauritania
  SS. Nigeria
  TT. Senegal
  UU. Tanzania
  VV. Tunisia
  WW. Algeria
  XX. Chad
  YY. DRC
  ZZ. Ethiopia
  AAA. Kenya
  BBB. Malawi
  CCC. Mauritania
  DDD. Niger
  EEE. Nigeria
  FFF. Rwanda
  GGG. Sierra Leone
  HHH. Swaziland
  IJJ. Tanzania
  KKK. Uganda
  LLL. South Africa
  MMM. Cameroon
  NNN. Ethiopia
  OOO. Kenya
  PPP. Malawi
  QQQ. Mauritania
  RRR. Nigeria
  SSS. Senegal
  TTT. Tanzania
  UUU. Tunisia

© Simmons & Simmons LLP 2014. Simmons & Simmons is an international legal practice carried on by Simmons & Simmons LLP and its affiliated partnerships and other entities.
Wide continental development

16 countries have already adopted a specific DP regulation
14 countries are publicly working on adopting a DP regulation

24 countries have not adopted any DP regulation yet
Law adoption dates

2001 Cap Verde
2003 Seychelles (not in force)
2004 Burkina Faso, Mauritius, Tunisia
2008 Senegal
2009 Morocco, Benin
2010 ECOWAS
2011 Angola, Gabon
2012 Ghana
2013 Mali, Ivory Coast, South Africa
2014 African Union, Comoros
2015 Madagascar
Focus on key jurisdictions

- Benin 2009
- Ghana 2012
- Tunisia 2004
- South Africa 2013
Tunisia (1/3)

Act No. 2004-63 of 27 July 2004 for the protection of personal data

- **Fully in force comprehensive data protection law with two implementing Decrees:**
  - Decree No. 2007-3004 dated 27 November 2007 on the conditions and processing of notification and authorization for the processing of personal data
  - Decree No. 2007-3003 dated 27 November 2007 on the functioning of the national authority for the protection of personal data: l’Instance Nationale de Protection des Données à Caractère Personnel (the “National Authority”)

- **Personal Data (“PD”)**
  - Any information, independently of its origin or format, identifying, directly or indirectly, an individual or rendering this individual identifiable, except for information pertaining to public life or considered as such by law.
  - The individual is considered as identifiable when she/he can be identified, directly or indirectly through several data or symbols concerning his/her identity, physical, psychical, genetic, social, economic, or cultural characteristics.

- **Data controller, data processor and their agents** must be a Tunisian national; reside in Tunisia and have no criminal records

- **Formalities**
  - Any processing of personal data is subject to a prior declaration or request of authorization to the National Authority.

- **Concept of sensitive data:** unless otherwise provided (e.g. authorization from the National Authority), the processing of personal data related, directly or indirectly, to racial or genetic origin, religious convictions, political, philosophical or trade-union related opinion or health is forbidden
Tunisia (2/3)

Act No. 2004-63 of 27 July 2004 for the protection of personal data

Key processing principles

- Processing shall respect human dignity, privacy and public liberties
- Data Collection shall be exclusively carried out for lawful, specific and explicit purposes
- Processing shall be loyal and within the limits of the collecting purpose(s)
- PD shall be accurate, precise and updated
- PD cannot be processed for other purposes unless when:
  - Data subject has given his/her consent
  - Processing is necessary to the safeguard of a vital interest of the data subject
  - Processing is necessary for scientific purposes
- The data controller shall take all appropriate measures to ensure the security and confidentiality of the PD

Data subject rights

- Shall give his/her consent (unless otherwise provided by law) and be fully informed of the processing
- Right of access, rectification and opposition

Restrictions on international transfers

- A data cross-border transfer is only possible when the country where the recipient is located provides for an adequate level of protection
- Cross-border transfer must be authorized by the Data Protection national authority
Tunisia (3/3)

Act No. 2004-63 of 27 July 2004 for the protection of personal data

- **Administrative measures** - The National Authority may withdraw the authorization or ban the processing notified after interviewing the data controller

- **Civil liability** of the data controller in case of violation of the Act

- **Criminal Sanctions**
  - Act of 27 June 2004 provides for several detailed sanctions, including:
    - **Illegal transfer of data abroad** that could cause harm the public security or Tunisian vital interests (including attempt) is punished by **2 to 5 years imprisonment and a fine ranging from Dinar 5,000 to 50,000** (about USD2,600 to 26,000)
    - **Processing PD despite a prohibition** (for instance sensitive data) is punished by **2 years imprisonment and a fine of Dinar 10,000 dinars** (about USD5,200)
    - **Obtaining the data subject consent illegally** by fraud, violence or threat is punished by **1 year imprisonment and a fine of Dinar 10,000** (about USD5,200)
    - **Keeping processing PD in spite of an opposition from the data subject** is punished by **1 year imprisonment and a fine of Dinar 5,000** (about USD2,600)
    - When the offender is a legal entity, the above-mentioned penalties are enforceable **against the manager** when his/her liability has been established
Benin (1/3)

Law No. 2009-09 of 22 May 2009 for personal data protection

- Relevant Data Protection Body: the National Commission for Technology and Freedoms (the “CNIL”)

- Personal data
  - All information related, directly or not, to an identified or identifiable individual by reference to an identification number or several other elements that are particular to that individual.
  - The identification is made through means available or one that can be accessible to the data controller or any other person

- Formalities
  - Unless otherwise provided by law, prior declaration to the CNIL or “recording of the data in a register kept by a person designated by the data controller” is required for PD processing that is managed by public or private organisations
  - Prior authorization of the CNIL is required for the processing of data notably related to a national identification number, biometry, health, offense, security defence of the State, interconnection of files with different purposes, and cross-border transfers

- Concept of “sensitive data”: Unless otherwise provided by the law (e.g. when data subject gives his/her express consent), collection of sensitive data is forbidden
Benin (2/3)

Law No. 2009-09 of 22 May 2009 for personal data protection

- **Key principles** – Personal data must be:
  - Collected and processed in a **loyal and lawful manner**
  - Collected for **specific, explicit, legitimate and not fraudulent purpose**
  - **Not be subsequently processed** in a manner **incompatible** with the **specific purpose declared or authorized**
  - **Appropriate, relevant and non-excessive** in light of the purpose for which they have been collected
  - **Truthful, accurate** and, if necessary, **updated**. If the data collected is false or incomplete the data controller must correct it
  - **Not be stored longer** than what is necessary for the purpose of the processing

- The data controller must take all **necessary precautionary measures** to insure the **security of the PD** including by preventing distortion, alteration or unauthorized intrusion

- **Data subject’s rights**
  - **Opposition** to any processing for legitimate purpose **AND** to **marketing processing for any reason**
  - **Information** regarding the processing, access to the data related to him/her and rectification

- **Restrictions on international transfers**
  - Transfer of PD abroad requires a **sufficient level of protection** in the country where the recipient is located
Benin (3/3)

Law No. 2009-09 of 22 May 2009 for personal data protection

- **Administrative sanctions by the CNIL** (appeal before the competent administrative jurisdiction)
  - **Warning or Formal notice** to comply with the Law within a maximum of 8 days
  - When the data controller *does not comply with the formal notice*, the CNIL may order:
    - **Monetary sanction** (proportional to the gravity of the breach)
    - Injunction to enjoin the data controller to **stop the processing**
    - **Withdrawal of the authorization**
    - **Locking access to certain personal data**
    - **Additional injunction** to proceed with the modification or the erasure of data and/or publication of the decision

- **Compensatory damages** may be granted to data subjects

- **Detailed Criminal offenses which notably include**:
  - Interfering with the CNIL’s work
  - Processing PD, even by negligence, without complying with the formalities provided by the Law
  - Processing sensitive data, related to prior criminal offenses or national identification number, without complying with the Law
  - Processing PD by fraudulent, disloyal or illegal means

- The criminal offenses are punishable by a fine ranging from **CFA franc 10 to 50 million** and/or by a **5 to 10 years imprisonment**
Ghana (1/3)

Data Protection Act No. 843 of 10 May 2012

- Relevant Data Protection Body: the **Data Protection Commission** (the “DPC”)

- **Scope** - The Act applies when:
  - Data controller is established in Ghana and the data is processed in Ghana. An unincorporated joint venture or association operating in part or in whole in Ghana is considered as established in this country
  - Data controller is not established in Ghana but uses equipment or a data processor carrying on business in Ghana to process personal data, or
  - Data processing in respect of information which originates partly or wholly from Ghana.

  The Data Protection Act does not apply when the data is originated externally and merely transits through Ghana

- **Personal data** – Data about an individual who can be identified:
  - From the data, or
  - From the data or other information in the possession, or likely to come into the possession of the data controller.

- **Registration** with the DPC is mandatory
  - Prior to processing PD (unless specific exemption like for: national security, research, crime and taxation purposes)
  - Not incorporated **data controller** in Ghana shall **register as an external company**
Ghana (2/3)

Data Protection Act No. 843 of 10 May 2012

- **Concept of sensitive data** – Referred to as “*Special Personal Data*”
  - The data controller **may not process special personal data** unless otherwise provided by the Data Protection Act

- **Key principles** - The data controller shall take into account the privacy of the individual by applying the following principles:
  - **Accountability**: Prior consent of the data subject, unless when it is necessary for the purpose of a contract to which the data subject is a party; the data shall be collected directly from the data subject
  - **Lawfulness of processing**: The data controller shall ensure that the personal data is processed without infringing the privacy rights of the data subject, in a lawful and reasonable manner. The data controller shall respect foreign personal data and ensure the compliance of the processing with the data protection legislation of the foreign jurisdiction
  - **Specification of purpose**: Personal data may only be processed if the purpose is necessary, relevant and not excessive and for a specific, explicit and lawful purpose that should be disclosed to the data subject. Personal data may not be processed for a period longer than necessary to achieve the purpose for which the data was collected.
  - **Compatibility of subsequent processing with the purpose of collection**
  - **Quality of information**: The data controller shall ensure that the data is complete, accurate, up-to-date and not misleading in consideration of the purpose for the collection or processing of the personal data.
  - **Openness**
  - **Data security safeguards**: Necessary steps to secure the integrity of PD through the adoption of appropriate, reasonable, technical and organisational measures to prevent loss of, damage to, or unauthorized destruction; and unlawful access to or unauthorized processing of PD. It shall ensure as well that any subcontractor or data processor complies with the security measures specified under this Act.
  - **Data subject participation**: Right for Data subject to access information and to correct it
Ghana (3/3)

Data Protection Act No. 843 of 10 May 2012

- There is no specific provision related to the international transfer of data

- Enforcement – The DPC may:
  - Issue an enforcement notice to a data controller who has contravened or is contravening any of the data protection principles, requiring the data controller to do any of the following: (i) to take or refrain from taking the steps specified within the time stated in the notice; (ii) to refrain from processing any personal data of a description specified in the notice; or (iii) to refrain from processing personal data or personal data of a description specified in the notice for the purposes specified or in the manner specified after the time specified
  - Upon request, make an assessment of the processing of PD

- Civil sanctions
  - Where an individual suffers damage or distress through the contravention by a data controller of the requirements of the Act, that individual is entitled to compensation from the data controller for the damage or distress
  - Specific additional remedies for data processed by Credit bureau (Credit Reporting Act, 2007)

- Criminal sanctions
  - A non-registered data controller who processes PD commits an offence which is punishable by a fine up to 250 "penalty units" and/or up to 2 years imprisonment
  - A data controller who fails to comply with an enforcement or information notice commits an offence and is liable on summary conviction to a fine up to 150 "penalty units" and/or up to one year imprisonment
  - A data controller, who purchases, obtains or discloses data subject's PD commits an offence and is liable on summary conviction to a fine up to 250 "penalty units" and/or up to two years imprisonment
  - A data controller who sells or offers to sell data subject's PD commits an offence and is liable on summary conviction to a fine up to 2,500 "penalty units" and/or up to 5 years imprisonment
Protection of Personal Information Act No. 4 of 26 November 2013

- Relevant Data Protection Body: the **Information Regulator** (the “**Regulator**”)

- **Scope** – This Act applies to the processing of personal information:
  - Entered in a record by or for a **responsible party** (data controller) by making use of automated or non automated means, provided that when the recorded PD is processed by non automated means, it forms part of a filing system
  - Where the responsible party is: **domiciled in South Africa**; or not domiciled in South Africa, but **makes use of automatic or non-automatic means in the country**, unless those means are used only to forward personal information through South Africa

- **Personal information**: Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person

- **Formalities**: The data controller must obtain an **authorisation** from the Regulator prior to any processing if it plans to:
  - Process any unique identifiers of data subjects for a **purpose other** than the one for which the identifier was specifically intended at collection and with the aim of linking the information together with the information processed by other responsible parties
  - Process information on **criminal behaviour or on unlawful or objectionable conduct** on behalf of third parties
  - Process information for the purposes of **credit reporting**
  - **Transfer sensitive data** ("**special person information**") or personal data related to children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information
  - Other types of information processing by law or regulation if such processing carries a **particular risk for the legitimate interest of the data subject** and if the Regulator decides that an authorization should be granted
South Africa (2/3)

Protection of Personal Information Act No. 4 of 26 November 2013

- General principles for lawful processing of personal data
  - **Accountability** for the data controller (« responsible party »)
  - **Processing limitation:**
    - Personal information must be processed lawfully, in a reasonable manner and must be adequate, relevant and not excessive given the purpose for which it is processed,
    - Data subject must give his/her consent, and
    - Personal information must be collected directly from the data subject except in some cases such as information being available to the public, prior consent to the collection of the information from another source, collection of the information from another source is necessary
  - **Purpose specification:**
    - Personal information must be collected for a specific, explicitly defined and lawful purpose to a function or activity of the responsible party
    - Except otherwise provided by law, records of personal information must not be retained any longer than is necessary
  - **Subsequent processing limitation** shall be in accordance or compatible with the purpose for which the data was collected
  - **Quality of information:** Data controller must take reasonably practical steps to ensure that personal information is complete, accurate, not misleading and updated where necessary
  - **Openness:** meaning maintaining the documentation of all processing operations under its responsibility and notifying to data subject when collecting personal information
  - **Security safeguards:** Data controller must secure the integrity and confidentiality of the information, and prevent loss or unauthorized destruction of the information
  - **Data subject participation:** Right for Data subject to access information and to correct it
South Africa (3/3)

Protection of Personal Information Act No. 4 of 26 November 2013

- Transfers of personal information outside of South Africa are prohibited, subject to exceptions

- 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
  - 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 USD843,215) may be imposed as an alternative to a criminal sanction
  - The relevant 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
  - 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 months
  - 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 months
  - Failure to comply with enforcement or information notices is punishable by a fine and/or an imprisonment for a period not exceeding 10 years
Key expectations

Trends in data protection regulations 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

- **Several legislations** rendering pan-African project difficult to implement

- **Great Influence of EU regulation** on data protection laws in the continent
  - 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:
      - Kenya public government’s open data webpage [https://opendata.go.ke/](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
Key expectations

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

- **Major 1st step**: for the first time, at a continent scale, 53 African 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
Simmons & Simmons has an alliance with leading US firm Seward & Kissel LLP for hedge fund and asset management work.

*Sociedade Rebelo de Sousa in association with Simmons & Simmons LLP
**Hamad & Al-Mehdar in alliance with Simmons & Simmons
Christophe Fichet
Avocat à la Cour / Partner
Simmons & Simmons LLP
DD +33 (0)1 53 29 16 56
cchristophe.fichet@simmons-simmons.com