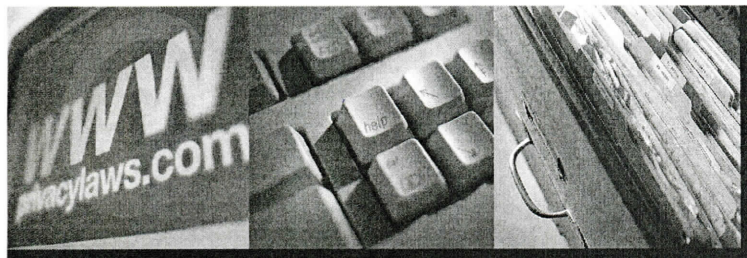

25 YEARS
PL&B ANNIVERSARY
1987-2012

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

FEDMA concerned about EU proposal's impact on marketers

The EU draft DP Regulation is too restrictive, says Mathilde Fiquet, EU Legal Affairs Adviser at FEDMA. Core issues are at stake for marketers. **Laura Linkomies** reports.

FEDMA's (the Federation of European Direct and Interactive Marketing) main concerns about the proposed EU Draft DP Regulation are a broadening of the definition of data subject, changes proposed to the lawfulness of processing, and restrictions to profiling. The organisation has been involved in the consultation process for the past two years in order to ensure that there is no legal uncertainty, and that self-regulatory measures are also included.

"There is an imbalance in the current proposals – the decisionmaker needs to better understand how the direct marketing industry works," Fiquet said. "The regulation has been drafted to address online issues and a

Continued on p.3

China: NPC Standing Committee takes a small leap forward

Graham Greanleaf explains a recent legislative provision from the National People's Congress Standing Committee which deals with personal data online.

The Decision of the Standing Committee of the National People's Congress (NPC Standing Committee) of 28 December 2012 concerning data privacy and the Internet[1] (2012 Decision) is the highest level law yet enacted in China to deal specifically with data protection issues. It is effective immediately[2].

The Standing Committee is the second-highest legislative organ in China, after the full NPC, and has extensive legislative powers[3]. As a sub-set of the membership of the NPC, it meets a number of times per year, whereas the full NPC is only in session annually. Decisions (jueding)

Continued on p.4

Issue 121 **February 2013**

NEWS

2 - DPAs cooperate more

8 - Critical times for EU DP proposal

13 - Ireland's DPA enforcing cookie law

16 - EU Art. 29 DP WP recommends limiting implementing acts

22 - EU declares that New Zealand's Privacy Act is 'adequate'

23 - Stricter breach notification in EU cyber security draft Directive

30 - Sony fine indicates 'appropriate security' • Dutch and Canadian DPAs challenge WhatsApp • California's mobile privacy guidelines

31 - US FTC fines Path $800,000 and launches mobile app guidance

ANALYSIS

12 - Australia's Privacy Act: Weaker principles, more enforcement

14 - Singapore's new DPA: Increased powers and business risk

26 - Asian privacy scholars explore social networking dangers

LEGISLATION & REGULATION

7 - India: Push for comprehensive act

10 - Italy legislates on call centres

24 - Kenya's Data Protection Bill 2012: Many leaks still unplugged

28 - Taiwan's PIPA into force, with controversial sections removed

MANAGEMENT

17 - Privacy in the cloud: Myths, facts

28 - Events Diary

29 - Book Reviews

31 - *PL&B's* Premium Access Service

Kenya's Data Protection Bill 2012: Many leaks still unplugged

The Bill is considerably weaker than any of the data privacy laws adopted by African countries so far. By **Alex B. Makulilo**.

On 10 January 2012, Kenya's Commission for Implementation of the Constitution (CIC) published a revised draft Data Protection Bill 2012. This draft Bill is currently undergoing internal review and stakeholders' consultation. Prior to that, the Ministry of Information and Communications for Kenya had issued a Data Protection Bill in June 2009. The need to adopt a data protection law in Kenya can partly be explained against the following background. First there are the cyber law reforms in the East African Community (EAC) in which Kenya is a member.[1] These reforms which culminated in the adoption of the East Africa Community Legal Framework for Cyberlaws Phase I in 2010 recommended the EAC member states to adopt data protection legislation based upon international best practices.[2] The second reason is the adoption of the Constitution of Kenya in 2010 which incorporates a provision for privacy.

Limited scope

The draft Bill applies to personal information held by public and private bodies described as both "agency" and "data controller" (s.2). Similarly, the scope of the Bill extends to both automatic and manual processing (long title of the proposed Bill). Yet there is no exemption of processing of personal data by a natural person in the course of personal or household activity. This means that a mere act of creating phone book contacts will amount to processing personal information (as defined in s.16) under Kenya's law. Moreover, the Bill does not provide for the usual exemptions for processing solely for journalistic, artistic and literary purposes. Surely this restricts these activities even if the public interest is overwhelming. Processing for purposes of the National Security Intelligence Service is partly exempted and there are also exemptions in the area of criminal law and law enforcement.

Extra-territoriality

The draft Bill does not provide any rule as to its territorial application. Although it may be generally assumed that the Bill intends to apply to data controllers established in Kenya, it is far less clear if that extends to the use of equipment in Kenya by a controller who is not established there. This may turn Kenya into a data heaven where personal data may be transferred in avoidance of stringent rules from other countries. However, the positive element of the Bill is that it affords protection to data subjects irrespective of their nationalities.

Weaker data protection principles

The draft Bill contains data protection principles similar to those provided in international codes of data privacy. These include lawful collection, purpose specification, minimisation, information quality, accuracy, access to information, correction, security, data retention and disclosure of information (Part II). However, in many places the scope and ambit of these principles fall short of the standards of international codes on data privacy. For instance, the Bill does not require processing to be fair. Similarly, the Bill does not provide for erasure, deletion, blocking or destruction after a data subject has gained access to his or her personal information. Moreover, most of these principles have many exemptions.

> The draft Bill applies to personal information held by public and private bodies described as both "agency" and "data controller".

Principles for specific types of processing

Sensitive personal data: The draft Bill has neither a definition nor regime for sensitive personal information. Yet it lists most of the known sensitive personal data in the definition of personal information, including information as race, sex, ethnic or social origin, colour, physical or mental health, religion, belief, culture, etc. [s.2 (1)(a)].

However, privacy in the area of HIV/Aids is specifically regulated by the Kenya's HIV/AIDS Prevention and Control Act 2006 (Act No.14 of 2006). One of the objectives of this Act is to guarantee the right to privacy of the individual [s.3 (b)(i)]. Particularly section 14 requires consent of an individual to HIV testing while section 18 treats results of HIV test as confidential information. To consolidate these provisions, the HIV/AIDS Prevention and Control Act empowers the Minister for health to make privacy guidelines to regulate confidentiality in the context of HIV testing and disclosure of results (ss. 20, 21, and 22). The Act makes it clear that any person who breaches any provision of the privacy guidelines made by the Minister shall commit an offence (s.23). The penalty for this breach, if no other punishment is provided, is imprisonment for a term not exceeding two years, or fine that does not exceed one hundred thousand shillings or both (s.43). Also the HIV/AIDS Prevention and Control

Act establishes a specialised court the HIV and AIDS Tribunal also known as the Equity Tribunal to deal with all complaints arising from the Act except for the complaints of a criminal nature (ss. 25 and 26). The Tribunal has powers to make various orders, award damages or costs [s.27 (7)].

Direct marketing: The draft Bill does not cover unsolicited marketing. Yet provisions for privacy protection in direct marketing are found in the Kenya Information and Communications (Consumer Protection) Regulations 2010. These regulations prohibit unsolicited direct marketing without the consent of a consumer [17(1)(2)]. However, direct marketing is permissible in the context of sale of goods or services where the marketer had legally obtained the contacts from the consumers and subsequently markets his or its similar goods or services to them [Regulation 17(3)]. In such cases, a consumer must be afforded an opportunity to reject marketing free of charge and in a simple manner [s.17 (3)]. Generally, the regulations provide that all automated direct marketing in Kenya shall be based upon the opt-in principle.

Automated decision making: The draft Bill lacks specific provisions dealing with automated decision-making involving personal data. This will subject individuals to schemes in which they will not only not understand the logic of their operation but which will also affect their legitimate interests.

Onward transfer restrictions

The draft Bill does not restrict onward transfer of personal information outside Kenya. This renders the Bill irrelevant for two reasons. First, while it purports to protect personal data, it at the same time makes it possible for such data to be transferred overseas without any protection. Second, in terms of business, the Bill is not helpful in making Kenya a secure location in as far as business process outsourcing (BPO) is concerned.

Independence of the Commissioner

The draft Bill does not establish a data protection commission. However, it makes cross-reference to the Commissioner in the Freedom of Information Bill 2012 as also the Commissioner of data protection [s.2 (1)]. The provisions of the Freedom of Information Bill (FOI) clearly show that the Commission is independent. The Commission is established as a body corporate [s.4, FOI]. Its independence is statutorily guaranteed (s.8 FOI). This means that the Commissioner is to function without political bias or interference, and must be wholly independent and separate from the government, any political party, nominating authority or any person or body. Moreover it is independent and not subject to the direction and control of any person or authority [s.8 (2)(b)FOI]. The Commissioner is only subject to the Constitution and the law [s.8 (2)(a)FOI]. Members of the Commission are appointed by the President but are subject to the approval by the Parliament [ss.9 and 11(7) FOI].

Compensation, injunctions and offences

The Commission may award damages for pecuniary loss, loss of any benefit, humiliation, loss of dignity and injury of the feelings as a result of interference with the personal data of an individual (s.23). It may similarly make declaratory orders and issue injunctions (s.22). There are also a range of offences under the draft Bill (s.26).

Enforcement

The draft Bill fails to clearly define the relationship between the High Court of Kenya and the Commission. For example, the Bill provides that 'a person whose rights have been breached under this Act shall have recourse before the Court (defined as the High Court in the Bill) [s.3 (2)]. At the same time, the Commission deals with similar complaints arising from the draft Bill.

Poor drafting

The draft Bill suffers from poor drafting. For example, section 3 provides for data protection principles. Surprisingly, section 4 similarly deals with principles and objects of data protection. The marginal notes to the two sections are sharply different: "principles of data protection" and "objects of data protection" respectively. Yet a closer look at these provisions reveals that section 3 provides the constitutional basis of the proposed Bill which seeks to implement Art 31 of the Constitution of Kenya 2010. Similarly, section 4 does not at all list any object of the Bill. Instead, it outlines the basic principles of data protection. Another illustration of confusing formulation is s.4 (1)(e). There are also a significant number of repetitions in the Bill. All in all, poor drafting is likely to result in interpretation difficulties of the law once enacted.

Conclusion

Kenya's draft Bill on data protection represents a weak standard of data protection legislation in Africa. As highlighted, there is no significant improvement between the 2009 draft Bill and the revised draft Bill 2012. Only two provisions (i.e. ss.3 and 4) have been added. As the draft Bill is still subject to consultation, there is enough opportunity to improve it. One way is to learn from the experience of other African countries with comprehensive data protection legislation as well as international best practice. If the Bill becomes law in its present form, Kenya's law will undermine cross-jurisdictional transfer of personal data across Africa and outside. It may similarly fail to live up the 'adequacy' standard of the European Directive 95/46/EC.

AUTHOR

Alex B. Makulilo is Lecturer at the Open University of Tanzania and PhD graduand, University of Bremen.
Email: kulwath@yahoo.co.uk

INFORMATION

1 Other members of the EAC include Uganda, Tanzania, Rwanda and Burundi.
2 Recommendation 19, Draft EAC Legal Framework for Cyberlaws 2008 (adopted on 7 May 2010 by the 2nd Extra-Ordinary Meeting of the EAC Sectoral Council on Transport, Communications and Meteorology).