

## PRESS RELEASE



**ISACA Kenya Chapter**  
**P.O Box 10384 - 00100**  
**Vision Plaza 3rd Floor Suite 4**  
**Tel: +254 (20) 2493578**  
**Mobile: +254 (786) 249357**  
**email: [info@isaca.or.ke](mailto:info@isaca.or.ke)**  
**Web: [www.isaca.or.ke](http://www.isaca.or.ke)**  
**Twitter: [@isaca\\_kenya](https://twitter.com/isaca_kenya)**

*ISACA-Kenya Comments on Freedom of Information and Data Protection Bills.*

### **The Organization**

ISACA Kenya Chapter is a Professional body of around 1,000 members. The members are professionals dealing in Information Security, IT Governance and Assurance. The Kenya Chapter is part of ISACA-International, the global body that deals in Information Security, IT Governance and Assurance.

### **The Task.**

The Commission for the implementation of the Constitution of Kenya (CIC) has published various bills (<http://www.cickenya.org/>) and invited public comments on the same. ISACA-Kenya commissioned a Task Force to review the Freedom of Information and the Data Protection Bills with the objective of contributing views on the same.

### **The Process**

ISACA-Kenya selected five members to constitute the Task Force which commenced work by reviewing Data Protection Acts and Freedom of Information Acts from various countries that included Mauritius, South Africa, India, Malaysia, UK,US amongst others. The Task-force benchmarked the Bills against the Seven Principles of Data Protection as defined by the European Union (EU) Data Protection Directive as outlined below.

- Notice—data subjects/citizens should be given notice when their data is being collected;
- Purpose—data should only be used for the purpose stated and not for any other purposes;
- Consent—data should not be disclosed without the data subject's consent;
- Security—collected data should be kept secure from any potential abuses;
- Disclosure—data subjects should be informed as to who is collecting their data;
- Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
- Accountability—data subjects should have a method available to them to hold data collectors accountable for following the above principles

**The Outcome.**

Whereas the two bills represented a good beginning as far as addressing data privacy and protection issues of the public in the digital age, the task force observed the following key aspects that needed to be addressed. The first one regards the clause that says that the enactment of the Data Protection Bill would not incur additional Public Funds. This is worrying because it may imply that the tasks foreseen in the Act in terms of regulation, enforcement and/or administration may not be eventually funded leading to an Act that is non-operational.

The second observation is that the Bill does not explicitly define the professionals who would be considered qualified to perform some of the roles within the Data Protection Act. Such roles include ensuring that organizations that deal in citizen data - both in private and public organizations - are keeping such data secure, up to date and with integrity. Furthermore, the Act does not explicitly oblige these organizations to perform and report on regular Information Security Audits - without which the Freedom of Information and Data Protection Commission would have no mechanism for regulating the Data Protection space.

The third and final key observation relates to the qualifications of the membership of the Freedom of Information and Data Protection Commission. Whereas it identifies potential candidates as being from the legal, business, corporate governance amongst other backgrounds, it does not mention people from Information Security backgrounds. We feel this would be necessary as data protection issues are getting more sophisticated in nature as technologies evolve over time.

**R. Akalah**  
**President, ISACA-Kenya.**