Attn: Mr. Jerome Ochieng
Principal Secretary, ICT &Innovation
Ministry of Information Technology and Communication,
Teleposta Towers
P.O. Box 30025-00100 NAIROBI

Attn: Chairperson
Taskforce on Development of the Policy and Regulatory Framework for Privacy and Data Protection in Kenya.
Communication Authority of Kenya
P.O. Box 14448 NAIROBI

We Savannah Training Solutions Limited did attend the session held on 2nd October 2018 and have reviewed the Bill and Policy however, both documents are silent as regards training of data controllers' workforces—which is a noteworthy omission.

Our proposed points are;

- Articles 39 and 47 of the GDPR require awareness and training, but these provisions are not in the Bill or Policy
- HIPAA in the USA has always required training of all staff
- Draft South Africa POPIA Regulations published for comment in South Africa last year added a provision for "awareness sessions [for staff]"
- Section 33(1)(c) of the Bill ascribes responsibility for public awareness to the Commission this public awareness campaign will need to be developed, deployed, and maintained.
- Section 15 of the Bill describes security measures, by which it may be inferred that security awareness training is to be provided (for example, reference section 7 (e.g., 7.2) of the ISO27001 standard).
- Section 8.2 of the Policy spells out the data controller's obligations, and 8.2.10 requires the development of policies and procedures—but nowhere is the data controller required to train its staff, which is a huge omission. Policies and proc dudes without staff training are pointless.
- Similarly, section 8.2.8 requires the appointment of a Data Protection Officer (DPO), but says nothing about their background, training, reporting relationship, independence, etc., which is covered in Articles 37, 38, and 39 of the GDPR. These are very important requirements, else

companies will appoint a junior person without the necessary training who doesn't report sufficiently high in the organisation to be effective.

- Section 8.3 should likewise require training for staff, especially software developers, on Privacy by Design, etc., or these requirements can't be met.
- Sections 11.2 and 11.5 of the Policy cannot be effective in preventing or deterring breaches if the information gathered is not communicated back to the staff of the organisation. There's no point reporting to the Regulator, and not advising staff internally of the risks, and taking action(s) to mitigate those risks. All of these activities should feed into an on-going and active awareness programme within the organisation.
- Section 8B2.1(b)(4) of the United States Sentencing Commission's elements of an Effective Compliance and Ethics Program, upon which most Compliance programs in the USA are based, includes the requirement for an organisation to train its staff on its policies and procedures, etc. This is one of only 7 elements listed, hence its high level of importance.

In order for Kenya to achieve a positive "adequacy" opinion from the European Data Protection Board, I respectfully submit that a number of the above points, if not all, need to be addressed. Especially critical is the need to capacity building by means of training cadres of qualified Data Protection Officer's (DPOs) who can take their new skills and knowledge back to their organizations, and spread the word. This will help the Commission's task of public awareness enormously as well.

We look forward to fruitful discussion on the proposed policy and bill.

Yours faithfully,

Dennis Mbai Njuguna

Executive Director

Savannah Training Solutions Limited

P: +254 20 2000687 M: +254 722 790377

A: 4th Floor Cavendish – 14 Riverside, Riverside Drive

W: www.savannahtraining.co.ke E: dennis@savannahtraining.co.ke