REVIEW OF THE DATA PROTECTION REGULATIONS 2022

Data Protection is fast taking a place of prominence in terms of regulating the caprices of the dynamic digitalized world we now find ourselves in. Further to the Cyber and Data Protection Act [ Chapter 12:07] which was promulgated with the policy objective of data privacy and protection of all data collected by Data Controllers both within and outside Zimbabwe depending on the location of the means used to process the said data. The life blood of any business operation is the collection and utilization of data, primarily collected from its stakeholders (usually customers/clients). The Cyber and Data Protection Act seek to shield the privacy of such information and regulate the way in which such information is stored, used and disclosed. To this end the Postal Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) has published the draft Data Protection Regulations 2022 and called upon the public to provide feedback on the suitability thereof. This article will briefly look at some of the provisions of the draft regulations and assess of the suitability or appropriateness thereof.

In terms of clause 3 of the draft regulations any person, entity or public agency, authority or other body, which determines the purposes and means of processing data, either alone or in collaboration with another, is required to obtain a data protection license to perform such tasks pertaining to personal data. The regulations currently provide that Data Controllers are supposed to take a self assessment test in terms of the licensing eligibility tool available from the regulatory authority’s website. While there might be merit in the self assessment tool and the same exercise a global standard, these authors opine that a more stringent test may be required particularly as issues of data privacy and data protection gain traction within Zimbabwe. It is further suggested if the regulations do not change the risk of a laxity in the licensing of Data Controllers would become an elevated business risk that might impede on the seamless movement and utilization of collected data for the purposes the same has been collected for. Clause 4 outlines various tiers of license categories for Data Controller and each respective license is linked to the organisations minimum annual gross turnover. The minimum annual gross turnover’s indicated start from USD 500 000-00 for a tier 1 data protection license up to an annual gross turnover of USD 1 000 000-00 for a tier 3 data protection license. The gross annual turnovers highlighted in the draft regulations may not necessarily reflect the business reality of the average business operating in Zimbabwe whose business model will be subject to the dictates of the Cyber and Data Protection Act. In effect with the increase in digitalized platforms and the collection of personal data at so many stages during the life cycle of a transaction in a digitalized world, it is fair to expect these draft regulations shall be applicable to the regular local business operations whose gross annual incomes do not even range within the range of the stratospheric amounts contained within the draft regulations. These figures betray the intent of making the Cyber and Data Protection Act wide ranging in scope and a law of general application. In effect the figures are discriminatory and yet it is plausible to envision every operational business wherein personal data is collected shall require a data protection license to continue in business.

The few clause highlighted above show the importance of the call for engagement with the draft regulations and appropriate feedback relayed back to POTRAZ to consider the relevant amendments. Whilst the consultative process in ongoing is must become apparent to business operators or whomsoever collects personal in the course of their enterprise that with the enactment of data protection regulations, the Cyber and Data Protection Act would have received the necessary mechanics to become fully operational. It is therefore pertinent to conclude with a word of caution that should one not have enacted an internal data protection policy aligned to the relevant Act, it may become necessary to do so to avoid the risk of penalties and other sanctions.