WERKSMANS ATTORNEYS

REGULATORY

Data protection impact assessment required despite "Might of the State"

1 December 2021 *6 min read*

Kenyan High Court

Introduction

On 14 October 2021, the Kenyan High Court declared the collection of biometric information and the rollout of the country's digital ID system "*Haduma cards*" unconstitutional.[1] The High Court cited that the National Integrated Identity Management System disregarded data protection frameworks, including the failure to conduct a data protection impact assessment ("**impact assessment**") as required in terms of the Kenyan Data Protection Act of 2019 ("**Data Protection Act**").

The judgement highlights two important issues that we in South Africa can take guidance from, namely that –

- the Protection of Personal Information Act 4 of 2013 ("**POPIA**") applies to state entities; and
- it is important to conduct an impact assessment in relation to an organisation's processing of personal information.

State entities are not exempt from complying with data protection legislation

In the South African context, state entities must comply with POPIA. Section 1 of POPIA provides that a public body is also a responsible party for purpose of POPIA. POPIA therefore equally applies to public and private entities. State entities must take cognisance of this and implement data privacy governance structures.

POPIA furthermore states that in terms of the interpretation and application of the Act, one could take into account international standards. This is clear from section 2 of POPIA which provides that one of the primary purposes of POPIA is to ensure harmony with international standards on data privacy. Therefore, the approach of the Kenyan court is something that state entities should take note of.

The Kenyan High Court clearly stated that state entities are not exempt from complying with data privacy legislation and there is a positive duty on them to implement data protection frameworks in line with data protection legislation.

Impact assessments

From a South African perspective, one of the core responsibilities of an Information Officer is to conduct an impact assessment to ensure that adequate measures exist to comply with POPIA.[2] Consequently, an impact assessment is compulsory in terms of POPIA.

So, what is an impact assessment and, what can be achieved from an impact assessment?

In essence, an impact assessment is a process to help an organisation identify and minimise the data protection risks arising from the organisation's processing of personal information.

It is good practice to conduct an impact assessment for processing that is likely to result in a high risk to the data privacy rights of individuals.[3] For example, when processing involves special personal information,[4] conducting an impact assessment would be prudent. In addition and specifically from a data security perspective, it is also good practice to conduct an impact assessment for any other major project which requires the processing of personal information.

An impact assessment must –[5]

- describe the nature, scope, context and purpose of the processing;
- assess the level of compliance with POPIA;
- identify and assess risk to individuals; and
- identify measures to mitigate against those risks.

However, even though not all risks can be eliminated from an impact assessment, an impact assessment most importantly enables an organisation to identify and mitigate against data protection risks, plan for the implementation of solutions to those risks and assess the processing activities of the responsible party.

Impact assessments give effect to the data "protection by design" principle[6] in that it assists with –

- putting in place appropriate technical and organisational measures designed to implement the data protection principles effectively; and
- integrating safeguards into processing activities so that an organisation meets the requirements for compliance and protects individual rights.

In this light, an impact assessment helps with improving the design of the processing activities and enhances an organisation's communication about data privacy risks with relevant stakeholders. Some of the benefits of an impact assessment include, amongst other things, –

- reducing data protection risks from processing activities; and
- reducing operation costs by optimising information flows and eliminating unnecessary data collection and processing.

Ultimately, conducting an impact assessment will improve the awareness of the data protection risks arising from an organisation's processing activities or a particular project.

Conclusion

The decision of the Kenyan High Court is a win for privacy and will hopefully shape and inform the public debate regarding the importance of complying with data protection legislation on the part of state entities. In addition, the judgement also highlights the importance of an impact assessment, especially in light of digital ID systems as they rapidly proliferate around the world.[7]

Digital ID systems require the collection of a vast amount of personal information (including special personal information). As a consequence, digital ID systems are inherently high-risk due to the nature of the information they include and the potential consequences for people.[8] A recent data breach to a digital ID database in Argentina compromised the personal information and credentials of an entire population.[9]

The vast collection of information required for digital ID systems implies equally vast civil and human rights considerations. In this digital age, data protection legislation is becoming increasingly central to the protection of these human rights, particularly rights of privacy.

Werksmans has bespoke products aimed at assisting your organisation in complying with POPIA. These products include a robust electronic impact assessment. Please contact us for further information.

Read more about POPIA: A Guide to the Protection of Personal Information Act of South Africa.

by Ahmore Burger-Smidt, Director and Head of Data Privacy and Cybercrime Practice and member of the Competition Law Practice; and Dale Adams, Associate

---

[1] *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology and 3 Others,* Judicial Review Application No. E1138 Of 2020

[2] See Regulation 4(1)(b) of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013): Regulations relating to the Protection of Personal Information.

[3] See "Data protection impact assessments" available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/, accessed on 21 November 2021. Also see "Data Protection Impact Assessment (DPIA)" available at https://gdpr.eu/data-protection-impact-assessment-template/, accessed on 23 November 2021.

[4] See section 26 of POPIA for the categories of special personal information.

[5] *Supra* note 2.

[6] Data "protection by design" emanates from the European Union's General Data Protection Regulation 2016/679 ("**GDPR**"). Also see "Data Protection Impact Assessment (DPIA)" available at https://gdpr.eu/data-protection-impact-assessment-template/, accessed on 23 November 2021.

[7] See "Kenyan High Court Ruling a Watershed Moment for Digital Rights" by E Renieris, available at https://www.cigionline.org/articles/kenyan-high-court-ruling-a-watershed-moment-for-digital-rights/, accessed on 21 November 2021.

[8] *Ibid.*

[9] See "Hacker steals government ID database for Argentina's entire population" by C Cimpanu available at https://therecord.media/hacker-steals-government-id-database-for-argentinas-entire-population/, accessed on 21 November 2021.

Ahmore Burger-Smidt

Head of Regulatory

View Profile