ENSafrica **webinar**

investing in Africa | Zambia

THU 24 AUG

speakers and key contacts

Mr Likando Luywa

Data Protection Commissioner | Zambia

Era Gunning

ENSafrica | Executive
Banking and Finance
egunning@ENSafrica.com
mobile +27 82 788 0827

Chipili Salati

Mulenga Mundashi Legal Practitioners | Partner
csalati@mmlp.co.zm
+260 211 254248/50

Q&A report

01. Transfer of data cross border: Does an organisation with a parent company outside of Zambia request authorisation in general or for every individual transfer process between the Zambia entity and the parent company?

If a Zambian company has a parent company located outside of Zambia and wishes to transfer personal data between the two, the requirement for authorisation depends on the circumstances:

1. **General Authorisation** - If the law permits certain types of data transfers between Zambia and the parent company without needing individual permissions, then the company might require general authorisation. This means they would have overall approval to transfer a specific category of data between the entities without needing separate permission for each transfer. This general authorisation can come from the Minister of Technology and Science ("the Minister"), who can prescribe permissible transfers outside the country.

2. **Individual Transfer Authorisation** - In other cases, such as when the data subject gives their consent or there is an urgent necessity, the company would need to seek authorisation from the Commissioner for each specific data transfer. This implies that they would need separate permissions for each instance of data transfer between Zambia and the parent company.

In essence, whether the company needs a single authorisation covering multiple transfers or specific permissions for each transfer depends on the circumstances and whether the law allows certain types of transfers without separate authorisation from the Commissioner or the Minister.

02. Does the Commissioner currently respond to advisory requests?

Yes, the Date Protection Commissioner currently responds to advisory requests.

03. Data protection representative: What are the requirements in respect of the position?

The requirements and qualifications for data protection representatives as well as those for auditors will be clarified in the Guidelines to be completed by October 2023.

Q&A report

04. Does the Data Protection Act No. 3 of 2021 ("**DPA**") anticipate a lot of requests for exceptions regarding the requirement to host data in-country and how does the office intend to deal with such requests? Can the Commissioner give an example where exemptions will be granted?

The DPA does anticipate that there might be requests for exceptions regarding the requirement to host data in-country. Section 70(2) allows the Minister to prescribe categories of personal data that may be stored outside the Republic. This implies that there could be instances where certain categories of data could be exempted from the requirement to host data in-country.

The Office of the Data Protection Commissioner, as outlined in the DPA, is responsible for approving standard contracts or intra-group schemes that allow data transfers subject to certain conditions. Additionally, the Commissioner can approve transfers based on necessity or due to compliance with specified criteria for cross-border data transfers under Section 71(2). The Commissioner is also tasked with monitoring circumstances applicable to data transferred outside Zambia and reviewing decisions made under the Act.

An example where exemptions could be granted is in the case of emergency situations where the transfer of data to a particular person or entity engaged in providing health services or emergency services is necessary (Section 71(4)(a)). Another example might be where the Commissioner is satisfied that transferring data to a particular international organisation or country adheres to the prescribed criteria and is necessary for specific data controllers or subjects, without hampering the effective enforcement of the Act (Section 71(4)(c)).

05. There needs to be much more sensitization about data access and usage. A lot of people in Zambia are ignorant about their Data Rights.

Yes, this is true. The Data Protection Commission (the "**Commission**") will put in place an extensive awareness programme not only for data subjects but also for data controllers, data processors and entities.

Q&A report

06. Data storage: What is the position if data is stored with a cloud service provider outside of Zambia?

According to the provided sections of the DPA, if data is stored with a cloud service provider outside of Zambia, the following points should be considered:

1. **General Rule** - Section 70(1) of the DPA mandates that personal data should be processed and stored on a server or data centre located in Zambia. This suggests that the default position is to host data within the country.

2. **Exceptions** - Section 70(2) allows the Minister to prescribe categories of personal data that may be stored outside Zambia. This implies that there could be circumstances or specific categories of data for which storing with a cloud service provider outside Zambia might be allowed based on the Minister's prescriptions.

3. **Cross-Border Data Transfers** - Section 71 addresses the transfer of personal data outside of Zambia. It outlines conditions under which such transfers are permissible. For instance, if the Minister has prescribed that transfers outside Zambia are permissible (Section 71(1)(a)(ii)), or if the Commissioner approves a transfer due to a situation of necessity (Section 71(1)(b)).

4. **Monitoring and Review** - The Commissioner is tasked with monitoring circumstances applicable to data transferred outside Zambia (Section 71(3)) and reviewing decisions made under the Act.

Given these provisions, the position regarding data storage with a cloud service provider outside of Zambia would depend on various factors, including the type of data, any prescriptions made by the Minister, and compliance with the conditions outlined in the DPA for cross-border data transfers. It is important to note that the Act provides for potential exceptions to the general rule of in-country data storage, but these exceptions are subject to specific conditions and approvals.

07. What qualifications, if any, will be prescribed for data protection officers?

Section 48 of the DPA stipulates that a data protection officer must be appointed following the guidelines issued by the Commissioner. It is important to note that the guidelines outlining the qualifications and requirements for data protection officers are yet to be issued by the Commissioner. Our interaction with the Data Protection Commissioner has revealed that it is unlikely that any qualifications will be prescribed at this stage.

Q&A report

08. Historical data: What is the expectation in respect of a data clean-up to comply with the minimality requirements?

Regarding historical data, as outlined in Section 51 of the DPA, the expectation is that a data controller and data processor should retain personal information for the duration it serves the specific purpose for which it was collected. Additionally, the data should remain relevant to that purpose. Furthermore, there is a stipulation to retain the personal information for a minimum of one (1) year beyond its relevance or any other period as stipulated.

To adhere to the requirements of minimal data usage, it is expected that historical data that no longer serves its original purpose should undergo a data clean-up process. This process involves periodic assessment by data controllers and data processors. If the data is no longer pertinent or necessary for its initial intent, it should be securely deleted or anonymised. This approach aligns with the principle of minimising data usage.

In conclusion, the expectation is that data controllers and data processors should regularly carry out data clean-up activities to ensure that historical data remains stored only for the necessary period and remains relevant to its original purpose. Unnecessary data should be appropriately disposed of to adhere to the minimal data usage principle established in the DPA.

Q&A report

09. Where data has been compromised, the DPA dictates that the subjects must be made aware. How practical is this and how does the Commission intend to monitor compliance to this?

The requirement within the DPA for data subjects to be informed in cases of data compromise is a pivotal aspect in upholding transparency and accountability in data protection. The practicality of executing this requirement relies on an entity's ability to respond promptly and effectively to such incidents. The Commission assumes a vital role in overseeing compliance with this provision.

To ensure practicality, entities are advised to establish well-defined protocols for detecting, assessing, and addressing data breaches. Swift incident response plans can help mitigate the impact of breaches and facilitate timely notifications to affected data subjects.

The Commission monitors compliance through various avenues, including:

1. **Reporting** - Entities are obliged to promptly notify the Commission about data breaches. This reporting enables the Commission to track incidents and ensure that appropriate actions are taken.

2. **Audits and Assessments** - The Commission may conduct audits or assessments of organisations to ascertain the presence of adequate data protection measures, including comprehensive incident response plans.

3. **Guidance and Enforcement** - The Commission provides guidance to organisations on optimal practices for managing and responding to data breaches. In instances of non-compliance, the Commission has the authority to enforce adherence to the law.

4. **Public Awareness** - The Commission's mandate encompasses raising public awareness regarding data protection. This includes educating individuals about their rights and outlining steps they should take if their data is compromised.

5. **Collaboration** - The Commission collaborates with various stakeholders, including government bodies and industry associations, to foster data protection practices and enhance compliance.

In summation, while the practicality of informing data subjects about breaches hinges on an entities preparedness, the Commission assumes a pivotal role in overseeing compliance. Through reporting, audits, guidance, enforcement, and collaboration, the Commission ensures entities meet the requirement of notifying data subjects in case of data compromise. This collective approach cultivates a more transparent and secure data protection landscape.

Q&A report

10. Can the consequences of data mismanagement be beyond fines?

Yes, the consequences of data mismanagement can indeed extend beyond financial fines and entities can face various other repercussions such as:

1. **Criminal Penalties** - In some cases, criminal penalties, including imprisonment, can be imposed for certain violations.

2. **Legal Action** - Individuals whose rights have been violated due to data mismanagement may take legal action against the entities for compensation or damages. For instance, failure to respect data subject rights (such as access, rectification, erasure, and portability) can result in legal actions and reputational harm.

3. **Regulatory Scrutiny** - Beyond fines, the Commissioner's office can subject entities to increased scrutiny, audits, or ongoing monitoring to ensure compliance.

4. **Corrective Measures** - The entities may be required to implement corrective measures, data protection audits, or regular assessments to address compliance gaps.

5. **Administrative Measures** - The Commissioner's office can impose a range of administrative measures beyond fines, including warnings, reprimands, and orders to cease specific data processing activities.

11. In this age of cloud-based information systems, how will the aspect of storing data in Zambia be handled particularly for companies that belong to groups that for cost purposes may have created one point of data storage for all its group companies? Making this a local entity obligation will increase the cost of doing business in Zambia and may be too costly for the local entities to manage alone.

These cases will be assessed on a case-by-case basis and determinations will vary based on the presentations made, agreements in place and the impact.

12. Is there consideration for different regulations relating to startups in the tech space and small businesses in respect of data protection and privacy?

Yes, the Commission will in future consider having different regulations to address the unique needs and circumstances of startups and small business.

Q&A report

13. Okay, so there’s a balance between tort and criminality. That's fair enough.

Yes. The balance between tort law and criminality plays a crucial role in the realm of data protection and privacy regulations. This equilibrium ensures that a comprehensive legal framework is in place to address a wide range of scenarios.

Tort law deals with civil wrongs, allowing individuals who have suffered harm due to data breaches or privacy violations to seek remedies through legal channels. This approach focuses on compensating individuals for the harm they have endured and holds entities accountable for their actions.

On the other hand, criminal law steps in to address more severe violations and intentional wrongdoing. It enforces penalties such as fines and even imprisonment for intentional and egregious breaches of data protection regulations. This aspect of the legal framework serves as a deterrent and sends a clear message that intentional violations will not be tolerated.

By combining these two legal approaches, data protection and privacy regulations strike a balance between addressing individual grievances and maintaining broader societal interests. This comprehensive approach ensures that individuals' rights are protected, while also discouraging malicious behaviour that could undermine the trust and security of personal data.

14. On the topic of cross-border data transfers, what is the view of the Office of the Data Protection Commissioner on cloud computing and storage of data in the cloud where the cloud is hosted outside of Zambia? Are the Zambia Information and Communications Technology Authority (ZICTA) and the Office of the Data Protection Commissioner aligned on cross-border data transfers?

The Office of the Data Protection Commissioner will give final direction on cross-border transfers, but of course working along with other regulators. Again, this will be on a case-by-case application. Notably, this law may be new to Zambia but there are many references to help provide guidance on the best practice on cross-border transfers.

Q&A report

15. These "exceptions" need to be regulated closely because some entities will find a loophole in these exceptions where our data can be exported (and sold) outside the country.

Certainly, the necessity for vigilant regulation of these "exceptions" is of paramount importance due to the potential for certain entities to exploit these provisions as loopholes. Without adequate oversight, there is a risk that these exceptions could be misused to facilitate the export and potentially sale of personal data outside Zambia.

To safeguard against such misuse, it is imperative for the Commission to closely monitor and enforce the application of these exceptions. By implementing robust criteria, rigorous evaluation processes, and regular audits, the Commission can ensure that data transfers adhere to the intended purposes and comply with the law. Transparency in the approval process and the establishment of clear guidelines for the exceptions can also contribute to preventing any deceptive practices.

The provisions of the DPA, particularly Sections 70 and 71, offer a framework for legitimate data transfers while maintaining data security and individuals' rights. By maintaining a watchful eye on the implementation of these exceptions and taking proactive measures to prevent potential exploitation, regulatory bodies can mitigate the risk of data being exported and potentially commercialised under misleading pretexts. This proactive stance ultimately aims to strike a balance between facilitating legitimate data transfers and safeguarding against any potential misuse or unauthorised disclosure.

16. Chipili, one of the challenges I recently faced was the implementation of the Authentication Act which requires documents signed outside Zambia to be authenticated. How is the Electronic Communications and Transactions Act (ECTA) reconciled with this Act? This is in relation to e-signatures.

While electronic signatures are recognised in Zambia, it is always safe to ensure that perhaps the time and dates are inserted to ensure that the last place of signature is in Zambia to deal with authentication issues, bearing in mind that the courts in dealing with authentication have always done so in the context of wet ink signature. In practice, in attempt to also deal with this issue, we have introduced a deeming clause on the counterparts clause to expressly ensure that the place of execution is Lusaka, Zambia as guided by the Supreme Court.

17. Mr Luywa, what is the approach of your office to cloud computing?

The new dispensation is about cloud computing and the Office of the Data Protection Commissioner encourages cloud computing but within the ambits of the law.