Deloitte.

Data Privacy:
How organisations can play their part in ensuring data privacy.

April 2023 | Deloitte Namibia Thought Leadership

MAKING AN IMPACT THAT MATTERS since 1845

Introduction

Data privacy is a component of data protection focused on personal information and keeping it safe against improper access, theft, or loss. Data is a valuable asset for organizations as it is used to make key decisions and provide a competitive advantage. It is however just as valuable to potential malicious attackers who wish to gain access to sensitive data. It is therefore critical for organizations to keep data confidential and secure by exercising sound data management practices and Implement controls to prevent unauthorized access and loss of data.

Every organization is responsible for ensuring sufficient controls are in place to ensure the security of the data they collect from their customers. It is therefore imperative that management within organizations understand these responsibilities and ensure the prioritization of data protection controls.

This article has a look at data privacy within the Namibian context and how organizations can ensure sufficient data protection controls are in place.

"Data privacy is a component of data protection focused on personal information and keeping it safe against improper access, theft, or loss."

How is data privacy currently governed?

There are various data protection regulations in the world that have been put in place to protect people's privacy and dictate the responsibilities of the organizations that may collect such data. An example would be the **General Data Protection Regulation (GDPR)**, which is applicable to any organization in the world that collects, processes and stores data related to people in and from the EU. The regulation outlines how organizations should process and store personal information of individuals and requires companies to ensure that they are compliant with the regulation.

The **Protection of Personal Information Act (POPI Act)** was put in place in South Africa in 2013 to regulate the processing of personal information by organisations. The act established the minimum standards related to the processing of personal information and requires all organisations in South Africa to be compliant with the set standards. The implementation of this act has resulted in businesses needing to make changes to how they process, store, and discard personal information collected from customers. The act also requires organisations to report data breaches to the South African information regulator and notify the affected data subjects.

Our neighbouring Botswana have also implemented the **Botswana data protection law** in 2018 which similarly aims to protect the privacy of data subjects, preventing data breaches or minimising the impact of data breaches should they occur. The law requires organizations to obtain consent from individuals before collecting, using, or disclosing their personal information and to take reasonable measures to ensure the security and confidentiality of that information. The law also provides data subjects with certain rights, such as the right to access their personal data, and establishes a regulatory body, the Data Protection Authority, to oversee compliance with the law. Non-compliance with the data protection law can result in fines and other penalties.

There are a vast number of laws that regulate data privacy in the world, which vary in content, however the goal remains to protect the public interest.

The responsibility for Data privacy

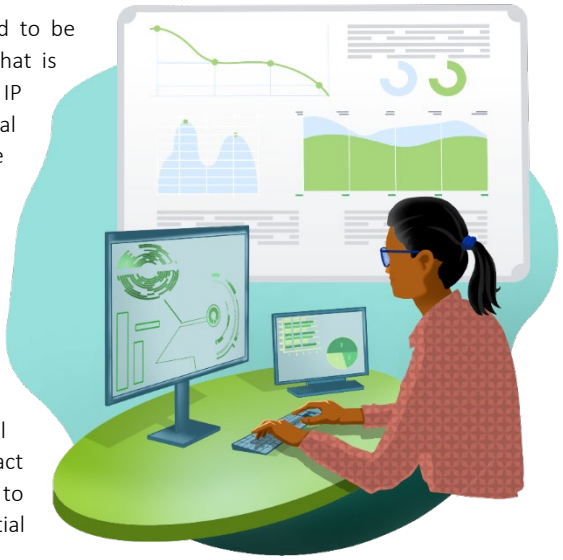
All organizations have a responsibility to protect the privacy of their customers' data. This includes implementing security measures such as encryption, firewalls, and access controls to prevent unauthorized access to sensitive information. Businesses should also have a clear data privacy policy that outlines how they collect, use, and share personal information.

Governments also have a responsibility to ensure data privacy by passing laws and regulations that establish the standards for the collection, processing, and protection of personal information. These data protection regulations provide a framework for organizations to ensure that they have implemented the controls necessary to protect personal information.

Individuals can also take steps to protect their data privacy by being mindful of the information they share online, using strong passwords, and regularly updating their security software. They should also be aware of their rights under privacy laws and take advantage of any tools that allow them to control the sharing of their personal information.

How may the draft Namibia data protection bill impact Namibian organizations?

The Ministry of Information and Communication Technology (MICT) published Namibia's draft Data Protection Bill in 2022 which will hopefully be passed into law soon. Like other existing bills, the proposed bill aims to establish a set of rules and principles to regulate the processing of personal information of Namibian citizens. It is the responsibility of Namibian organizations who collect, process and store personal data, to ensure they are familiar with this bill.



Namibian companies that collect, process and store personal data need to be aligned on the definition and understanding of what constitutes data that is private (e.g., Biometric data, health data, genetic data, personal data, IP (Internet Protocol) Address, Location data and note the reference to special personal data incl. religious, philosophical beliefs, race, ethnic origin, trade union membership, political persuasion, health or sex life and Criminal behaviour) and that which is not.

Namibian organisations should also note the restrictions and limitation on were collected data points be stored (as the draft bill proposes to strictly limit storage and processing of personal data to within the physical, geographical borders of Namibia, given some exceptions) and how it should be processed (e.g., automated individual decision making and "profiling."). This may impact how organisations make use of international third parties for the storage and processing of collected data and may impact existing cloud strategies. It is therefore beneficial for organisations to familiarise themselves with the proposed regulations and assess the potential impact should the bill be passed into law.

Namibian organizations may also need to consider the recruitment of a Data Protection Officer (DPO) or formally assign this responsibility to someone with similar expertise in the organization, who will be responsible for ensuring compliance with Data Protection regulations.

The proposed data protection bill, if passed into law will be beneficial to both individuals and organisations in Namibia as it will result in improved data protection practices across the country and will build public trust in compliant organisations that collect and process personal information.

What are the business Risks and Consequences of poor data privacy controls

The consequences of a data breach are far-reaching and may have a major impact on any entity's ability to continue in operation. The immediate consequences are an inability to operate until the breach is contained, additional effort required to address regulatory compliance deficiencies, protecting customer information post the breach and performing public relation activities to minimize the impact of the event.

Apart from the potentially extensive costs of cyber investigations and remediation, attorney fees and litigation costs, there may be an increase in insurance premiums and the cost to raise capital directly attributable to a breach.

On the intangible side, costs of a data breach include the inevitable devaluation of the trade name, loss of customer confidence and potential loss of intellectual property, which directly translates to lost future revenues. Customers and employees are increasingly becoming aware of the amount of data being gathered about them and are becoming more mindful about choosing to engage with companies with a strong track record of data privacy.

There is therefore a strong incentive to manage data privacy and cyber security concerns upfront, which helps minimize crisis management and future-proofs the business.

"Customers and employees are increasingly becoming aware of the amount of data being gathered about them and are becoming more mindful about choosing to engage with companies with a strong track record of data privacy."

What are the benefits of data protection initiatives?

Data protection is important to maintaining the confidentiality, integrity and availability of personal data collected by organizations. Strong data security controls build a relationship of trust between organizations and their customers. Customers are more likely to do business and willingly submit their personal data to organizations that have a reputation for protecting personal data. These organizations that prioritize data protection may gain a competitive advantage with increased customer trust and loyalty. Another benefit of data protection laws is the reduction of cyber-attacks through the strengthening of IT and information security controls.

Emerging technologies such as the internet of things, cloud computing and big data have presented data loss risks considering the large amounts of information that are processed as a result. It is critical to the benefit of the public interest that appropriate data protection laws are in place to minimize the potential risk of cyber-attacks and such laws provide an appropriate framework for the development of new technologies.

How can you protect your valuable customer data?

Protecting customer data is a critical aspect of conducting business in today's digital age. The following are some steps organizations can take to protect customer data:

- Enforce strong password security on data processing and storage systems.[1]
- Appropriately classify data and make use of encryption to secure sensitive information, such as credit card numbers or personal information.
- Store customer data in secure, encrypted databases and limit access to those who need it through role-based access controls.
- On a regular basis, perform IT and information security audits to identify and address potential vulnerabilities within their environment.
- Provide information security training to employees regularly to ensure they understand their responsibilities to keep information secure.
- Ensure good patch management practices in the organization to prevent cyber breaches.
- Use firewalls, antivirus software, and other security tools to protect against cyber-attacks.
- Have a disaster recovery and incident response plan in place to quickly respond to a data breach or other security incidents.
- Monitor access to customer data and track all changes.
- Establish clear privacy policies and communicate them to customers.
- Establish data retention policies to manage the collection, storage, and disposal of data.

By taking these steps, companies can help ensure that customer data is protected from theft, loss, or unauthorized access.

In conclusion, data privacy is a critical issue that affects individuals, businesses, and governments. While businesses and governments have a responsibility to protect personal information, individuals also play a critical role in safeguarding their own data privacy. By working together, we can ensure that personal information is protected and used responsibly.

---

[1] NIST recommended Password Requirements:

- Length: Passwords should be at least 8 characters in length. However, there is no maximum length recommendation.
- Complexity: Passwords should be composed of a mix of characters, including uppercase and lowercase letters, numbers, and special characters. However, the guidelines suggest that complexity requirements should be abandoned in favour of length requirements.
- Composition rules: Passwords should not contain commonly used words, phrases, or patterns, or personal information that is easily guessable.
- Blacklist: Passwords should be checked against a blacklist of commonly used passwords and should not be allowed if they appear on the list.
- Two-factor authentication: Two-factor authentication should be used whenever possible, to provide an extra layer of security beyond a password.

About the Authors

Paulus Imene
IT Audit assistant manager
Mobile: + 264 81 407 9786
Email: pimene@deloitte.co.za

Melanie Harrison
Director RA (Risk Advisory)
Mobile: + 264 81 224 0899
Email: melharrison@deloitte.co.za

Deloitte.