Botswana Institute of Banking & Finance

Transforming future capability

2024 DATA PROTECTION Conference

REPORT

SecuringData,ProtectingPrivacy: Strengthening Data Protection Practices in Botswana

CPD CERTIFIED

The CPD Certification Service

The content of the following has been certified by
The CPD Certification Service as conforming to
Continuing Professional Development principles

NATIONAL DATA PROTECTION CONFERENCE 2024
Event: 5-6 December 2024

MEMBER

BOTSWANA INSTITUTE OF BANKING AND FINANCE
(017724)

Date:
January 2025

Certificate No:
61325

The CPD Certification Service, Boston House,
69-75 Boston Manor Road, Brentford, London TW8 9JJ
E-mail: info@cpduk.co.uk Web: www.cpduk.co.uk
Tel: 020 8840 4383

Copyright © 2025

All material in this document is the property of the **Botswana Institute of Banking and Finance**. Full **copyright** and other intellectual property laws protect these materials. Reproduction or retransmission of this manual, in whole or in part, in any manner, without the prior written consent of the Botswana Institute of Banking and Finance as **copyright** holder, is a violation of **copyright** law. Users may not distribute such copies to others, whether or not in electronic form, whether or not for a charge or other consideration, without prior written consent of the Botswana Institute of Banking and Finance.

Offenders will be prosecuted under the appropriate intellectual property laws as enacted by the Republic of Botswana.

Botswana Institute of Banking and Finance
Private Bag 00404
Gaborone
Botswana
Tel: (267) 3952493
Fax: (267) 3904307
Email: enquiries-academics@bibf.ac.bw
www.bibf.ac.bw

FOREWORD

By: Mr Molaodi Menyatso (*BIBF Acting Managing Director***)**

I am pleased to present to you the report on the proceedings of the Data Protection Conference hosted by the Botswana Institute of Banking and Finance on the 5th and 6th of December 2024, at Phakalane Golf Estate Hotel and Convention Centre under the theme, "Securing Data, Protecting Privacy: Strengthening Data Protection Practices in Botswana". The event attracted and brought together 230 key players across various sectors responsible for generating, using and maintaining personal data and ensuring the privacy of individuals in relation to their personal data.

The digital revolution has brought unprecedented opportunities and challenges, particularly concerning data protection and privacy. As Botswana advances in its digital transformation journey, ensuring robust data protection practices has become an imperative. To that end, the event sought to explore the intricacies of data protection in an increasingly digital world.

In today's information-driven economy, data is one of our most valuable assets. The importance of safeguarding this asset has never been more critical. As we witness rapid technological advancements, the rise of digital transactions, and the proliferation of personal data, the issues surrounding data privacy and security assume paramount significance.

The purpose of the event was therefore to facilitate a national dialogue on strengthening personal data protection practices in Botswana and to explore available avenues and practical solutions to prevent and mitigate the dangers of non-compliance to the individual, the organization and the broader economy.

The conference brought together leading experts, practitioners, and key decision-makers from various fields to share insights, best practices, and innovative solutions in data protection. The diverse range of panels and presentations enabled delegates to engage deeply with compliance with emerging regulations, the implementation of effective data governance strategies, and the impact of technological advancements on data security.

Furthermore, the event served as a platform for networking and collaboration. The exchange of ideas among diverse participants fostered a collective understanding of the shared challenges we face and inspired us to develop proactive strategies to address them. Participants' constructive engagements with the speakers and the panelists clearly demonstrated that, together, we can build a stronger framework for data protection that benefits not just our organizations, but also the society we serve.

BIBF is therefore particularly grateful for the support extended from the Ministry of Office of the President and the Data Protection Commission office for making this event a memorable one.

I would also like to express my heartfelt gratitude to our kenynote speaker Professor Sizwe Snail, our sponsors, our presentors, our partners, and the organizing committee for their relentless efforts in making this conference a reality. I encourage all attendees to reflect on and share their experiences, and envision a future where data protection is not just a regulatory requirement, but a cornerstone of trust and innovation in our organisations.

Molaodi Laxton Menyatso
BIBF Managing Director

TABLE OF CONTENTS

Foreword ..... i - ii
Executive Summary ..... iii - iv
Acronyms v

DAY 1 PROCEEDINGS / SESSION 1

Welcome Remarks :by Mr Molaodi Menyatso (*BIBF Managing Director*) ..... 2 - 3
Opening Remarks :*Speech given by Assistant Minister of State President,* Ms. Maipelo Mophuting 4- 6
Data Protection in Botswana : by Ms Ketshephaone Ngidi (Botswana Data Protection Commission) ..... 8 - 9
Keynote Address : by Professor Sizwe Snail *(Cyberlaw and AI Law expert, Admitted Attorney in South Africa and Former Member of Information Regulator, Contributor to South Africa POPIA Law)* ..... 10 - 11

SESSION 2

Presentation 1:Navigating the Botswana Data Protection Act: Key Insight and Compliance Strategies: by Ms Lebogang George *(Independent Consultant, Data Protection and Data Privacy Law expert)* ..... 13 - 20
Presentation 2 :Evolution of Data Protection Laws- Global Context: by Mr Kgotso Botlhole *(Managing Partner Botlhole LawGroup)* ..... 22 - 24
Presentation 3 :Data Protection Through the Lens of Judicial Decisions: by Ms Senwelo Modise *(Partner at Bookbinder Business Law)* ..... 26 - 28

SESSION 3

Panel Discussion: The Role of Data Protection in Media & Communication: (*Moderator*) Mr Fungai Mazarura *(Business & Public Relations Consultant)* ..... 30 - 32
Panel Discussion 2: The Future of Data Protection in the Age of AI and Big Data: *(Moderator)* Professor Sizwe Snail (*South African Cyberlaw and AI Law Expert)* ..... 33 - 36
Panel Discussion 3: Data Protection Compliance in the Digital Banking Age: *(Moderator)* Ms. Sedilame Modiga *(Manager, Business Compliance Advisory, Stanbic)* ..... 37 - 40

DAY 2 PROCEEDINGS / SESSION 4

Presentation 4: Implementation of Data Protection Laws in Ghana, Implementation & Enforcement as the First Data Protection Commissioner –Strides Made: by Dr Quintin Akrobotu (*Director, Regulatory & Compliance*) ..... 42 - 44
Presentation 5:GDPR as International Best Practice : by Mr. Paul Esselaar *(South Africa Admitted Attorney, Data Protection / Privacy Law, Researcher in ICT Solutions)* ..... 46 - 48

SESSION 5

Panel Discussion 4:Cybersecurity Law, Technology Law: *(Moderator)* Professor Sizwe Snail *(South Africa Cyberlaw and AI Law Expert)* ..... 50 - 52

Breakaway Session 1:

Leveraging Technology to Ensure Compliance and Implementation of Data Protection: by Mr. Fred Webb *(Compliance Lead, Debswana)*..... 54 - 56

Breakaway Session 2:

Compliance Readiness Checklist: by Ms. Senwelo Modise *(Partner at Bookbinder Business Law)*..... 57

SESSION 6

Panel Discussion 5: Data Protection in the Digital Age: *(Moderator)* Ms. Lebogang George *(Independent Consultant, Data Protection and Data Privacy Law Expert)*..... 59 - 62

Presentation 6: Bridging Borders: Botswana's Data Protection Bill in a Global Landscape: by Mr Paul Esselaar *(South Africa Admitted Attorney, Data Protection / Privacy Law, Researcher in ICT Solutions)*..... 64 - 65

Presentation 7:Contribution to the Successful Implementation of the Data Protection Act (DPA)-The Role of BoFiNet: by Shadrack Makhane *(Digital Delta Data Centre)*..... 67- 69

Closing Remarks: by Professor Nkobi Pansiri *(BIBF Council Member)*..... 70 - 71

Summary Highlights of the Conference..... 72

Implementation Challenges..... 73 - 76

CURRENT STATUS QUO OF THE BDPC (BOTSWANA DATA PROTECTION COMMISSION)

CHALLENGES EXPERIENCED AND ENVISAGED

Appendix 1..... 78 -81

Questions and Responses raised during the sessions

Appendix 2..... 82 - 86

Sample Compliance Readiness Checklist

NOTES:

Key Takeaways..... 87

Appendix 3..... 88 - 90

Conference Agenda

Executive Summary

The Botswana Institute of Banking and Finance hosted a Data protection conference from the 5th to the 6th December 2024. The conference is deemed crucial for the following reasons:

i.**Heightened awareness:** Increasing recognition of the importance of data protection and privacy.

ii. **Capacity building:** Addressing the need for enhanced capabilities in data protection practices.

iii. **Policy dialogue:** Fostering discussions on robust data protection policies and frameworks.

iv. **Collaboration:** Promoting partnerships and knowledge sharing among stakeholders.

v. **Empowerment:** Equipping individuals with the knowledge and tools to protect their data and privacy rights effectively.

The conference therefore provided an in-depth platform for discussing key issues surrounding data protection, compliance, and technology law in Botswana, focusing on the challenges and strategies for implementing data protection laws in the digital age.

The event brought together experts from the legal, cybersecurity, and compliance sectors to engage in discussions on topics such as artificial intelligence, big data, cybersecurity law, and the impact of evolving technological frameworks on data protection compliance. The conference further highlighted the importance of aligning local laws with international standards, such as the GDPR, to enhance the credibility and effectiveness of data protection frameworks.

It was emphasized that building a new regulatory body like the Botswana Data Protection Commission (BDPC) requires careful planning, resource allocation, and stakeholder engagement. Moreover, achieving successful implementation necessitates raising public awareness, as education and cultural shifts play a critical role in fostering a deep understanding of data protection rights and responsibilities.

Amongst the central themes of the conference was the role of technology in ensuring compliance with data protection laws. Several experts discussed how leveraging technology can improve compliance processes, enhance data protection measures, and support the implementation of new regulatory frameworks. However, the discussions also identified several challenges to implementation, including a complex regulatory landscape, resource constraints, and a lack of awareness and education among businesses and consumers. The limited technological infrastructure in Botswana was also highlighted as a significant barrier for companies trying to implement robust data protection systems.

The current status of the BDPC was discussed, noting that while the legal framework for data protection is in place, the Commission is still in the early stages of its operations and faces challenges in enforcement due to limited resources and technological capabilities. The BDPC's ability to monitor and ensure compliance is hampered by a lack of comprehensive guidelines on many aspects of data protection. The commission is actively working on building its capacity and raising awareness about the Data Protection Act, but significant challenges remain in educating both businesses and the general public.

As the deadline for full implementation of data protection regulations approached on January 13, 2025, the conference underscored the urgent need for action. Stakeholders highlighted the importance of strengthening BDPC enforcement mechanisms, issuing clear guidelines, and building the capacity of businesses to comply with the regulations. There was a consensus that leveraging technology solutions would be critical for businesses to meet compliance requirements. The risks of non-compliance, including legal penalties and reputational damage, were noted as major concerns, especially for businesses involved in the digital economy or those handling sensitive customer data.

The conference also addressed future challenges, such as the lack of alignment between

international and local laws, the shortage of skilled personnel in data protection, technological constraints, and cultural resistance to change within organizations. The discussions revealed that many businesses had yet to make substantial progress toward compliance, and the ambiguity in legal and regulatory frameworks remained a key issue.

In conclusion, the conference highlighted the importance of collaboration between the government, private sector, and regulatory bodies to ensure that Botswana met international data protection standards. The challenges faced by stakeholders, including limited resources and legal ambiguities, demonstrated the need for proactive planning and capacity-building efforts. By strengthening regulatory enforcement, providing clear guidelines, and fostering awareness, Botswana can ensure that its data protection framework supports trust and growth in the digital economy. However, without substantial efforts to address these issues, the risks of non-compliance could hinder progress.

"Delegates in attendance"

ACRONYMS

AI: Artificial Intelligence

BDPC: Botswana Data Protection Commissioner

BIBF: Botswana Institute of Banking and Finance

CJEU: Court of Justice European Union

DoJ: Department of Justice

DPA: Data Protection Act

DPbDD: Data Protection by Design and Default

DPIA: Data Protection Impact Assessments

DPO: Data Protection Officer

DPP: Data Protection Practices

GDPR: General Data Protection Regulations

POPIA: Protection of Personal Information Act

ROPA: Records Of Processing Activities

SAPS: South African Police Service

2024 DATA PROTECTION Conference
05-06 December

DAY 1 PROCEEDINGS:

Opening Prayer:
Mr Segomotso Mosokotso

5TH DECEMBER 2024

SESSION 1

- Welcome Remarks
- Opening Remarks
- Data Protection Insights and Background
- Keynote Address

Welcome Remarks

Theme: "Securing Data, Protecting Privacy: Strengthening Data Protection Practices in Botswana":

By: Mr Molaodi Menyatso (*BIBF Acting Managing Director***)**

Welcome Remarks by Mr Molaodi Menyatso

Mr Molaodi Laxton Menyatso, the Acting Managing Director of the Botswana Institute of Banking and Finance (BIBF), gave the welcome remarks to a diverse gathering of stakeholders, dignitaries, and participantst that set the tone for the conference themed *"Securing Data, Protecting Privacy: Strengthening Data Protection Practices in Botswana."*

Mr. Menyatso began by expressing his profound sense of responsibility and gratitude, welcoming all participants, including distinguished guests, sponsors, partners, and the esteemed Guest of Honour. He acknowledged their invaluable support and commitment to this critical issue, emphasizing the importance of their collective responsibility in advancing data protection practices in Botswana.

Highlighting the importance of data in today's digital era, Mr. Menyatso underscored its value as a critical asset. He stressed that as technology continues to evolve and reliance on data increases, protecting it and safeguarding individual privacy are essential to maintaining trust and integrity within organizations and the communities they serve.

Addressing the responsibility of industry representatives, he emphasized that data protection extends beyond mere compliance. He called for the establishment of a culture of privacy and security, to foster confidence among customers and stakeholders. This commitment, he explained, is the foundation for the conference's theme, which reflects the urgency and importance of the subject.

Mr. Menyatso described the conference as more than just a platform for discussion, calling it an opportunity for collaboration, learning, and the exchange of best practices. He encouraged participants to engage actively, challenge conventional thinking, and to explore innovative solutions to data protection challenges.

He expressed gratitude to the sponsors, partners, and delegates for their unwavering commitment to data privacy and security. Their presence, he noted, demonstrated a shared dedication to safeguarding sensitive information and upholding the privacy rights of individuals.

Outlining his expectations for the conference, Mr. Menyatso articulated several key objectives. He envisioned the event as a catalyst for change, innovation, and inspiration, providing a deeper understanding of the challenges associated with

data protection while identifying practical solutions to identified challenges . He reiterated BIBF's commitment to hosting similar conferences annually to address emerging financial and technological issues, reinforcing the Institution's dedication to fostering knowledge and skills development in banking and finance.

He emphasized the importance of collaboration, highlighting the role of all stakeholders in ensuring the conference's success. Their collective efforts, he stated, would contribute to building a safer and more secure financial environment.

Concluding his remarks, Mr. Menyatso warmly welcomed all participants and urged them to approach the conference with enthusiasm and purpose. He encouraged attendees to make the most of the opportunity, building connections and learning from one another. He expressed hope that the outcomes of the conference would lead to the development of resilient data protection frameworks capable of withstanding the test of time.

Through his remarks, Mr. Menyatso underscored the critical role of shared commitment, collaboration, and innovation in advancing data protection practices in Botswana, inspiring participants to actively contribute to this vital course.

Assistance Minister of President Ms Maipelo Mophuthing (on right) meeting some presenters

Opening Remarks

His Honor Mr Ndaba Gaolathe (Vice President of the Republic of Botswana & Minister of Finance): Speech given by: Assistant Minister of State President, Ms. Maipelo Mophuting

Opening Remarks by Ms. Maipelo Mophuting

The Assistant Minister of State President, Ms. Maipelo Mophuting, delivered opening remarks on behalf of the Vice President and stressed the significance of data protection in Botswana's evolving digital landscape and the collaborative effort required to advance data protection initiatives.

B.1. Key Highlights from the Speech

1. Importance of Data Protection
Ms. Mophuting stressed that data protection is a fundamental human right and a critical pillar for national security, integrity, and economic growth. She linked the adoption of robust data protection frameworks to Botswana's aspiration to position itself as a preferred investment destination.

2. Legislative Milestone: The Data Protection Act, No. 18 of 2024
The Minister highlighted the significance of the recently enacted Data Protection Act, which sets the foundation for safeguarding personal data while promoting economic innovation. She noted that the Act strikes a balance between enabling businesses to leverage data and protecting individuals' privacy rights.

3. Global Standards and Digital Transformation
The Minister said in line with international best practices, the government has established the Data Protection Commission to oversee compliance, promote awareness, and build capacity in both public and private sectors. She emphasized that integrating data protection into digital strategies is critical, especially in sensitive sectors like banking and financial services.

4. Digital Evolution and Cybersecurity Risks
She acknowledged the transformative impact of digital technologies on daily life, particularly in banking, with services such as online banking, mobile payments, and loyalty programs. However, she cautioned that these developments have heightened the risks of cyberattacks, making robust data protection measures imperative.

5. Compliance and Penalties
The Minister reiterated the penalties for non-compliance with the Data Protection Act, which include fines of up to P50 million or imprisonment of up to nine years. She clarified that the Act's intent is not punitive but preventive, encouraging organizations to uphold privacy as a fundamental human right to protect their customers and their organizations' reputations.

6. Role of BIBF and Stakeholders

Ms. Mophuting commended BIBF for organizing the conference, describing it as a critical step in fostering dialogue across sectors to strengthen Botswana's data protection ecosystem. She highlighted the need for collaboration among the government, private sector, and civil society to build a culture of compliance and public awareness about data rights.

B.2. Government Expectations from the Data Protection Commission

1. Implementation of the Data Protection Act
The Minister informed participants that the Commission is expected to ensure full compliance with the Act across all sectors, with a focus on protecting individuals' rights and fostering trust in Botswana's digital economy.

2. Capacity Building and Public Awareness
The Minister further implored the Commission to educate organizations and individuals about their responsibilities and rights concerning data privacy. This includes promoting awareness campaigns and training programs.

3. Collaboration and Knowledge Sharing
She opined that facilitating partnerships between the government, private sector, and international stakeholders is critical to staying ahead of emerging data protection challenges as illustrated by the data protection conference hosted by BIBF.

4. Cybersecurity Advocacy
Ms Mophuting also implored the Commission to work to minimize the risks of cyberattacks by advocating for advanced technological and administrative safeguards.

5. Monitoring and Enforcement
Ms Mophuting futher adjured the Commission to enforce compliance through regular audits and apply penalties judiciously to deter non -compliance while fostering a culture of doing the right thing.

6. Banking Sector's Role
The Minister underscored the banking sector's responsibility as custodians of sensitive personal and financial data. She urged financial institutions to adopt stringent data protection policies and technologies to maintain public trust.

7. Economic Implications
When addressing the economic implications for data protection, she said it is critical to driving Botswana's digital economy and ensuring its competitiveness in the global market. Therefore, the conference should be seen as an opportunity to chart a collective path toward a resilient and secure digital future.

8. Closing Thoughts
Ms. Mophuting reaffirmed the government's commitment to fostering a robust data protection culture and aligning with international standards. She encouraged participants from various sectors to engage in meaningful dialogue and collaboration during the conference to shape innovative and practical solutions for Botswana's data protection challenges. The conference, she noted, serves as a platform to safeguard the present, while building a secure future for all Batswana. She officially declared the conference open, emphasizing the collective responsibility to protect personal data and uphold the country's digital integrity.

(From left to right) -*BIBF Acting Managing Director (Mr Molaodi L. Menyatso) with Assistant Minister of State President, (Ms. Maipelo Mophuting), BIBF Council Member (Thelma Majela) and BIBF Council Member (Professor Nkobi Pansiri)*


2024
DATA
PROTECTION
Conference
05-06 December

Data Protection Insights and Background

PRESENTATION 1: Data Protection in Botswana

By: Ms Ketshephaone Ngidi (*Botswana Data Protection Commission)*

Presenter Ms Ketshephaone Ngidi

Ms Ngidi introduced the subject by highlighting that the establishment of the Information and Data Protection Commission in Botswana marked a significant step forward in addressing the need for privacy and data protection amidst advancing technological challenges. She noted that, created under Section 4 of the Data Protection Act No. 32 of 2018 (DPA), the Commission officially came into being following the Act's passing in Parliament in July 2018 and its assent in August 2018. However, it was not until October 15, 2021, that the Act commenced, signalling the beginning of Botswana's journey toward comprehensive data protection.

In February 2022, Mrs. Kepaletswe Somolekae was appointed as the Information and Data Protection Commissioner, tasked with spearheading the implementation of the Act and laying the foundation for the Commission's operations. The presentation covered the following key areas.

1. Challenges Faced by the Commission

Ms Ngidi highlighted that the introduction of the Data Protection Act presented both opportunities and significant challenges. The Act was intended to extend the reach of privacy laws to protect personal data processed both digitally and manually, making it essential to ensure its relevance amidst rapidly evolving technological advancements.

She said one of the initial tasks undertaken by the Commission was a thorough analysis of the Act to identify areas for improvement. This led to recommendations for aligning the Act with international standards, such as Convention 108 and the General Data Protection Regulations (GDPR). However, the implementation of the Act posed unique challenges, particularly as it required a cultural shift in how personal data is handled by data controllers and processors. This change necessitated education and a paradigm shift in businesses and organizations, emphasizing the inextricable link between operational processes and the use of personal data.

Additionally, the challenge of establishing a new institution from scratch added layers of complexity, including securing resources, recruiting qualified personnel, and setting up operational structures.

2. Advancements in Data Protection (2024)

Ms Ngidi further indicated that despite the initial hurdles, the Commission has made significant progress. She informed participants that the Act, which provides enhanced protection for data

subjects and broadens its scope, is set to fully commence in January 2025. She also announced that the Commission has established offices at Finance House in the Government Enclave and recruited staff to advance its mandate. Plans are underway to hire additional officers to strengthen its capacity further.

Moreover, the Commission is actively engaging with data controllers and processors to ensure compliance with the Act and the adequate protection of data subjects' rights. Public education has also been identified as a critical component of the Commission's mandate, aimed at raising awareness about data protection rights and responsibilities.

3. Key Features of the Updated Act (2024)

In her presentation, Ms Ngidi also informed the participants that the 2024 amendments to the Data Protection Act introduced several additional provisions that were not there in the original act to enhance its efficacy. Key highlights include:

3.1.**Extraterritorial Application:** The Act now applies to data controllers and processors outside Botswana, ensuring a global reach.

3.2.**Introduction of Administrative Fines:** Non-compliance attracts substantial penalties, including fines based on total worldwide turnover.

3.3 **Vesting of New Rights:** Data subjects are now afforded additional rights, such as the right to restriction, data portability, and objection to automated decision-making.

3.4.**Enhanced Obligations for Controllers:** Controllers must ensure data protection by design and default (DPbDD), maintain records of processing activities (ROPA), and conduct data protection impact assessments (DPIAs).

3.5.**Professional Standards for Data Protection Officers (DPOs):** Conditions for appointing DPOs now emphasize independence, qualifications, and duties.

4. Implications of Non-Compliance

Ms Ngidi noted that the Act introduces strict penalties for non-compliance, emphasizing the importance of adhering to data protection principles. Violations such as processing personal data contrary to legal provisions, mishandling children's data, or failing to implement appropriate security safeguards attract fines ranging from P500,000 to P50 million or imprisonment terms of up to nine years. Additionally, the sale of personal data is strictly prohibited, with severe penalties for offenders.

She further submitted that the introduction of the Data Protection Act and the establishment of the Information and Data Protection Commission in Botswana signal the country's commitment to safeguarding personal data in a digital age. She said while challenges remain, the collaborative efforts of all stakeholders—government, businesses, and individuals—will be critical in ensuring the successful implementation of the Act. She concluded by emphasizing the Commission's dedication to public education, international alignment, and rigorous enforcement as a promising step toward a data-secure Botswana.

Keynote Address

By: Professor Sizwe Snail (*Cyberlaw and AI Law expert, Admitted Attorney in South Africa and Former Member of Information Regulator, Contributor to South Africa POPIA Law***)**

*Keynote Address by **Professor Sizwe Snail***

Professor Snail kick started his keynote address by highlighting the right to privacy as a fundamental human right recognized and protected under Section 14 of the South African Constitution. This right ensures that individuals enjoy a sphere of autonomy free from unjustified interference, particularly concerning their personal information and private communications. He noted that, over the years, South African courts and the Protection of Personal Information Act (POPIA) have reinforced this right through landmark rulings, enforcement actions, and the imposition of legal obligations on responsible parties managing personal data. His keynote address focused on the following critical issues:

1. Judicial Definitions and Interpretations of Privacy

On judicial precedence, Professor Snail said the South African courts have provided valuable insights into the scope and application of privacy. He highlighted some cases related to the data protection law that were experienced in South Africa from which Botswana could draw some insights:

(i). **Khumalo and Others v Holomisa:** The court emphasized that privacy safeguards an individual's sphere of intimacy and autonomy from invasion.

(ii). **Bernstein v Bester NO AO:** This case highlighted the abstract nature of privacy, describing it as an "amorphous and elusive" concept.

(iii). **Mistry v Interim National Medical and Dental Council and Others:** The court concluded that the constitutional right to privacy does not cover information obtained non-intrusively, not related to personal life, used for its intended purpose, and appropriately disseminated.

(iv). **Black Sash Trust v Minister of Social Development and Others (2017):** The Constitutional Court ruled that SASSA must ensure personal data remains private, restricting its use to grant payments and purposes authorized by the Minister. This case underscored the importance of protecting beneficiaries' data from being exploited for marketing purposes without consent.

2. Protection of Personal Information Act (POPIA)

Prof Snail informed the audience that, POPIA is South Africa's primary legislation on data protection and was enacted to protect the personal information of data subjects. The act outlines eight conditions for the lawful processing of personal information:

i.Accountability

ii.Processing limitation

iii.Purpose specification
iv.Further processing limitation
v.Information quality
vi.Openness
vii.Security safeguards
viii.Data subject participation

3. Obligations Under Sections 19–22 of POPIA

He said under Sections 19–22, responsible parties have critical obligations to protect personal data, including:

i.Ensuring the integrity and confidentiality of personal information through technical and organizational measures.

ii.Identifying risks to personal information, maintaining safeguards, verifying their efficacy, and updating them regularly.

iii.Notifying the Information Regulator and affected data subjects in case of a data breach, taking immediate corrective actions.

iv.Delaying notification only if law enforcement determines it may impede investigations.

4. Notable Enforcement Cases

Several high-profile enforcement actions demonstrate the seriousness with which South African authorities handle violations of privacy laws. He emphasised that learning from these cases would empower Botswana Data Protection Commission and provide a smoother learning curve.

i). **Dis-Chem Pharmacy:** Following a data breach affecting 3.6 million records, the Information Regulator found Dis-Chem liable for using weak passwords, inadequate monitoring, and failing to notify affected individuals. The Regulator issued an enforcement notice directing Dis-Chem to improve its data protection measures and comply with POPIA.

ii). **South African Police Service (SAPS):** After victims' personal information was unlawfully shared on social media, SAPS was ordered to apologize publicly, investigate the members responsible, and comply with section 22 of POPIA regarding notification of data subjects.

iii). **Department of Justice (DoJ):** Following a 2021 cyberattack that exposed sensitive data, the DoJ was fined R5 million for failing to renew antivirus software and intrusion detection licenses, violating POPIA's security safeguards requirements.

iv). **FT Rams Consulting:** The company was penalized for sending unsolicited marketing communications without consent and failing to honour opt-out requests. It was instructed to cease the practice and develop a database of individuals who withheld consent for direct marketing.

5. Key Milestones Achieved

He further highlighted the key milestones that South Africa had attained to date. He also emphasises that the recent developments further reflect the growing importance of data protection in South Africa:

i.On 15 August 2022, the Information Regulator issued guidelines on reporting security compromises using prescribed forms.

ii.On 22 July 2022, the Regulator's inaugural Enforcement Committee met, marking a significant step in implementing POPIA.

His point of emphasis hinged on the urgency and importance of stakeholder engagement. He concluded by indicating that the right to privacy, as protected by the South African Constitution and POPIA, places stringent obligations on responsible parties to safeguard personal information. Enforcement actions against entities like Dis-Chem, SAPS, and the DoJ illustrate the country's commitment to holding parties accountable for breaches. These measures aim to ensure a robust data protection framework that upholds individuals' privacy rights while fostering trust in the digital era.

SESSION 2

Presentation 1

Navigating the Botswana Data Protection Act: Key Insight and Compliance Strategies:

Presentation 2

Evolution of Data Protection Laws- Global Context:

Presentation 3

Data Protection Through the Lens of Judicial Decisions:

Presentation 1

Navigating the Botswana Data Protection Act: Key Insight and Compliance Strategies:

By Ms Lebogang George (*Independent Consultant, Data Protection and Data Privacy Law expert***)**

*Presenter-**Ms Lebogang George***

Ms Lebogang George gave a comprehensive guide to the Botswana Data Protection Act (DPA) and outlined the specific roles and responsibilities of various organizational departments in ensuring compliance. The insights and strategies presented here underscore the importance of integrating data protection measures into everyday business processes to safeguard sensitive information, maintain trust, and drive sustainable growth.

1. Overview of the Botswana Data Protection Act

Ms George introduced her presentation by giving a background to the development of the DPA and the subsequent establishment of the Data Protection Commission. She highlighted that the DPA was promulgated in 2018 and effected in 2021 with affected entities given a grace period to comply with the ACT up to 15 October 2022. However, due to the low level of readiness of most entities, an extension was granted to 15 September 2023 followed by another to 13 January 2025. She opined that the Botswana Data Protection Act is a legal framework designed to regulate the processing of personal data while protecting individuals' privacy rights.

She said The Act provides clear guidance on compliance requirements for organizations, emphasizing transparency, accountability, and the ethical handling of data. She noted that with the advent of technology it has become much easier to transfer data and the DPA implementation would help with the regulation of information and data collection and storage to ensure the protection of data privacy. She urged organizations to implement policies and systems to manage personal data effectively while mitigating risks of breaches or unlawful access in respect for confidentiality and anonymity. To that end, Ms George brought the attention of the participants to the following DPA requirements.

i) Obligations under the DPA.

Ms George noted that there was need for entities to familiarise themselves thoroughly with the requirements of the DPA to ensure compliance with the Act and avoid unnecessary breaches. She outlined the following DPA obligations for all entities handling personal data.

- *Allowing Data Subject (tenants, buyers, suppliers, staff, clients, customers etc.) access to their Personal Data.*

- *Securely keeping Personal Data.*

•Training staff on the DPA.

•Cooperating with the Commissioner/Office of the Commission.

•Notifying the Commissioner/Commission of any data breaches.

•If a Data Protection Representative is appointed – registering them with the Commission.

•Collecting data in a lawful manner and as per the requirements and criteria set out in Section 14 of the DPA.

•Embedding privacy and data protection in every new innovation throughout the entire organization – privacy by design.

ii) The Rights of Data Subjects

Ms George further implored entities to be cognizant of the rights of data subjects when handling personal data and articulated them as follows.

1. The right to access Personal Data through subject access requests

2. The right to obtain a copy of the Personal Data obtained by a Data Processor of a Data Controller

3. The right to object, for legitimate reasons, to the processing of Personal Data concerning them

4. The right to oppose the processing of their Personal Data for direct marketing and

5. The right to correct, update, lock or delete Personal Data where it is inaccurate or incomplete.

2. Departmental Roles and Responsibilities

This presentation further highlights the roles of key departments for any organization to facilitate adherence to the DPA and ensure the protection of sensitive information, with a focus on compliance strategies, risk mitigation, and operational alignment.

a. IT Department

The IT department plays a pivotal role in building and maintaining a secure technological infrastructure to support data protection initiatives. Ms. Lebogang George emphasized the critical importance of safeguarding personal and organizational information in today's data-driven era. She highlighted that protecting data goes beyond mere compliance with regulations and is fundamental to building trust and ensuring operational resilience. Organizations, she noted, must adopt a comprehensive approach that integrates technological measures, policy frameworks, and human awareness to enhance data protection strategies and maintain secure and compliant operations.

One of the key practices Ms. George outlined was conducting gap analyses of existing IT systems. She explained that these assessments serve as diagnostic tools, helping organizations identify vulnerabilities and areas needing improvement. By comparing current systems with industry best practices, organizations can address shortcomings, whether through software updates, infrastructure enhancements, or advanced cybersecurity solutions. This proactive approach, she stressed, helps businesses anticipate and mitigate potential threats.

In addition, she underscored the importance of data audits in gaining a clear understanding of how personal data flows within an organization. By reviewing data processing practices and maintaining detailed records of personal data lifecycles, organizations can identify risks and inefficiencies. Ms. George pointed out that regular audits not only ensure compliance with data protection laws but also foster a culture of accountability, embedding data protection into everyday operations.

Ms George further emphasized the necessity of establishing a strong policy framework to support

technical measures. She advocated for the development of comprehensive policies, including Cybersecurity, IT and Business Continuity, and Cyber-Incident Response Management. These policies, she noted, provide a roadmap for addressing cyber threats, minimizing disruptions, and ensuring business resilience. She highlighted that clear guideline, such as those found in an Incident Response Policy, enable swift and effective action during data breaches, mitigating damage and restoring trust. Policies, she remarked, are the cornerstone of a robust data protection strategy, offering essential guidance to leadership and employees alike.

However, Ms. George cautioned that even the best policies and systems could fail without adequate employee training. She called for initiatives such as phishing simulations and interactive workshops to educate staff on identifying and responding to potential threats. Training programs, she explained, empower employees to act as the first line of defence against cyberattacks by recognizing suspicious activity, safeguarding sensitive information, and adhering to security protocols. Building a security-conscious workforce, she asserted, is vital to reducing human errors that could lead to data breaches.

Lastly, Ms. George highlighted the role of access control in safeguarding sensitive data. She advised organizations to restrict access to files containing personal information, ensuring that only authorized personnel can handle critical data. Additionally, she recommended clear guidelines on the secure use of cloud-based systems to protect offsite-stored data from breaches. Implementing measures like role-based permissions and multi-factor authentication, she explained, provides an extra layer of security, reducing the risk of unauthorized access.

Ms George stressed that effective data protection requires a multi-faceted approach, including gap analyses, data audits, policy development, employee training, and access controls. She reiterated that these measures collectively create a robust data protection environment, shielding organizations from cyber threats while building trust among stakeholders and customers. As the digital landscape evolves, she urged organizations to adopt proactive strategies to ensure their operations remain secure and sustainable. She further implored IT departments to IT develop cyber-incidents management plan, to conduct phishing simulations and educate employees on other forms of unlawful access to personal data. These practices, she concluded, are essential for maintaining compliance, safeguarding information, and fostering resilience in an increasingly interconnected world.

b. Finance Department

Ms George highlighted the critical role of the Finance Department in ensuring compliance with Data Protection Act (DPA) requirements, particularly in the management of sensitive financial data. She emphasized that the department must adopt stringent measures to align its practices with data protection policies.

She outlined the importance of auditing accounting software systems to confirm their compliance with established data protection standards. These audits, she explained, help identify potential vulnerabilities and ensure that financial systems are equipped to handle data securely, in line with regulatory expectations.

Ms George also stressed the necessity of maintaining accurate and secure data records. She noted that the Finance Department must process financial transactions securely while adhering to tax legislation. Proper record-keeping, she explained, is not only essential for legal compliance but also critical to protecting sensitive financial information from unauthorized access.

She said the Finance Department can ensure it fulfills its obligations under the DPA while safeguarding financial data and maintaining the trust of stakeholders.

c.Human Capital & Administration Department

Ms George underlined the pivotal responsibility of HR departments managing sensitive employee data in safeguarding personal information while maintaining transparency. She stressed the importance of implementing practices that align with data protection regulations to build trust and uphold employee rights.

She highlighted data retention as a key responsibility, advising that employee data should only be retained for the duration legally permissible. Furthermore, employees must be informed about the retention periods of their data to promote transparency and compliance with the law.

Ms. George also stressed the need for stringent access control measures to protect sensitive employee information. She recommended limiting access to files containing personal data, ensuring that only authorized personnel can handle such information, thereby reducing the risk of unauthorized use or breaches.

Additionally, she emphasized the importance of employee awareness regarding their data rights. She advocated for ensuring that employees are well-informed about their rights to access and understand the organization's data retention policies. This, she noted, not only empowers employees but also fosters a culture of accountability and trust within the organization.

She reiterated that by adhering to these practices like responsible data retention, robust access control, and fostering employee awareness all departments can fulfill their obligations under data protection laws while safeguarding the rights and privacy of their employees.

d. Legal Services and Strategy, Policy & Planning Department

MsGeorge outlined the critical role of the department in ensuring that organizational policies and contracts align with the Data Protection Act (DPA) while upholding the overall integrity of the organization. She emphasized the department's mandate to oversee compliance and act as internal regulators to maintain high governance standards.

She noted the importance of legal compliance, stating that the department must proactively identify legal risks, draft policies, and update contracts to reflect the requirements of the DPA. These efforts ensure that all organizational agreements and frameworks remain aligned with evolving data protection laws.

In terms of governance, Ms. George emphasized the department's responsibility to notify all relevant stakeholders of new legislation and its implications. She also stressed the importance of securing Board approval for compliance initiatives, positioning the department as an internal regulator tasked with preserving organizational integrity and aligning operations with legal standards.

Ms George further highlighted the necessity of policy implementation, encouraging the development of a comprehensive compliance policy that outlines all applicable laws and regulations. This policy, she explained, serves as a critical reference point for ensuring that organizational practices adhere to both national and international standards.

She reiterated that the Governance Department's proactive approach to legal compliance, governance, and policy implementation is essential for fostering a culture of accountability and protecting the organization from potential legal and reputational risks.

e. Risk and Compliance Department

Ms George highlighted the vital role of this department in ensuring organizational compliance while effectively managing risks associated with data protection. She emphasized the need to balance regulatory adherence with fostering trust among stakeholders. She said the department could be considered the internal police of the organisation and was vital for preserving its integrity.

Ms Georger further underlined the critical role of the department in ensuring that the organisation complied with laws, regulations and rules and cooperate with regulators. She highlighted the importance of conducting internal audits for risk assessment as a key compliance measure. These audits evaluate corporate governance and data handling processes within the organization to identify potential risks and areas of non-compliance with the DPA. Regular evaluations, she explained, help ensure that data management practices align with legal and regulatory standards

Ms. George also stressed the need for process optimization as part of the department's mandate. This involves identifying systems or practices that fail to meet compliance requirements and recommending targeted improvements. By addressing these inefficiencies, the organization can mitigate risks and enhance its overall adherence to data protection laws.

She opined that implementing a comprehensive data policy that sets out all laws, regulations and regulators that fall withing the realm of each entity's sector, the department plays a pivotal role in upholding compliance, safeguarding the organization's reputation, and fostering a culture of accountability and continuous improvement.

f. Marketing & Communication Department

Ms. Lebogang George also outlined the critical responsibility of this department in promoting the organization's work while ensuring strict adherence to the Data Protection Act (DPA). She emphasized the department's role in maintaining compliance and enhancing operational efficiency. She indicated that while she appreciated the critiacl role of the department in marketing and promoting the organisation and acting as a counduit for communication of the organisation's work, vision, strategy and goals, that it should do with the confines of the DPA.

Ms George underscored the importance of direct marketing compliance, referencing Section 18 of the Data Protection Act (DPA). She stressed that organizations must obtain explicit consent from individuals before processing their personal data for direct marketing purposes. This practice, she explained, not only ensures compliance with the law but also respects individuals' rights to privacy. She said compliance will require organisations to give the data subject the opportunity to "OPT-IN" or OPT-OUT"

She also emphasized the significance of stakeholder engagement as a key component of compliance efforts. Communicating the organization's adherence to the DPA, Ms George noted, helps build trust and credibility among clients, partners, and the public. Transparent engagement assures stakeholders that the organization prioritizes data protection and operates with integrity especially where data subject are informed of their right to revoke previous consent should the wish to do so.

Ms George reiterated that by aligning direct marketing practices with legal requirements and fostering open communication with stakeholders, the department plays a critical role in managing risks while enhancing the organization's reputation and trustworthiness.

g. Internal Audit Department

Ms George outlined the critical role of internal auditors in ensuring the organization maintains accurate records and complies with the requirements of the Data Protection Act (DPA). She emphasized the importance of their contribution to both data integrity and regulatory compliance.

She noted the necessity of data audits, highlighting that internal auditors must conduct regular reviews of stored and archived data. These audits are vital for identifying potential risks, ensuring data accuracy, and confirming that the organization's data management practices align with legal requirements. Regular audits, she added, are instrumental in maintaining accountability and preventing lapses in compliance.

Ms George also stressed the importance of policy

development as part of the auditors' responsibilities. She recommended the creation of a comprehensive Data Management Record Policy that aligns with both legal and regulatory standards. Such a policy serves as a framework for managing data throughout its lifecycle, from collection and storage to archiving and deletion, ensuring consistency and compliance across the organization.

She also noted that internal auditors, through their focus on data audits and policy development, play a pivotal role in safeguarding organizational compliance, fostering transparency, and supporting effective data governance.

She reiterated that through internal audits and process optimization, the department plays a pivotal role in upholding compliance, safeguarding the organization's reputation, and fostering a culture of accountability and continuous improvement.

h. Documents & Records Department

Ms. Lebogang George outlined the crucial role of the Documents & Records Department in managing sensitive archived data while ensuring adherence to data retention policies. She emphasized the department's responsibility in safeguarding organizational records and maintaining compliance with relevant legal frameworks.

She highlighted the importance of ensuring data integrity within the department. This involves maintaining secure storage systems for archived data and restricting access to files containing personal information. By implementing strict access controls and secure storage practices, the department helps protect sensitive data from unauthorized access or breaches.

Ms. George also emphasized the need for policy adherence as a core function of the department. She recommended the development of data retention policies that align with existing legal frameworks, such as the Employment Act and the Companies Act. These policies provide clear guidance on how long specific types of data should be retained and establish protocols for secure data disposal when retention periods expire.

She reiterated that by focusing on data integrity and policy adherence, the Documents & Records Department plays a critical role in ensuring compliance, preserving the confidentiality of archived data, and upholding the organization's legal obligations.

i. Procurement Department

When outlining the importance of the procurement department in data protection, she stressed the critical importance of the procurement team in managing sensitive supplier data and ensuring compliance with the Data Protection Act (DPA), with a focus on transparency in tender processes.

She highlighted the importance of supplier data protection, emphasizing the team's role in safeguarding information about suppliers, partners, and contractors. By protecting this sensitive data, the procurement team prevents potential financial loss and legal repercussions that could arise from data breaches or misuse.

Ms. George also stressed the importance of fair competition in the procurement process. She noted that maintaining the integrity of bidding data is essential for promoting fairness and transparency. Ensuring that all procurement processes are conducted without bias and with full transparency helps foster trust among suppliers and upholds the integrity of the organization.

Additionally, Ms. George emphasized policy alignment as a key responsibility. The procurement team should request bidders' Data Protection Policies and ensure that service providers comply with the DPA. This alignment ensures that all parties involved in the procurement process adhere to data protection standards, safeguarding personal and financial

information throughout the engagement.

Ms. George reinforced that through diligent supplier data protection, maintaining fair competition, and aligning with data protection policies, the procurement team plays a crucial role in ensuring the organization's compliance with the DPA, fostering transparency, and mitigating potential risks.

j. Board of Directors

Ms George stressed the importance of the Board of Directors as custodians of corporate governance in ensuring compliance with the DPA and protecting the reputation and integrity of their organizations. She outlined as one of the principles of governance the role of the Board in IT governance to ensure proper data governance and management of data assets. She emphasized the importance of the governing structures in determining and governing the strategic direction of their entities to ensure compliance and approve policies for data protection. She concluded by noting that when buy-in comes from the top a culture of compliance will be embedded in the organization.

3. Key Compliance Strategies

Ms George went on to propose several key compliance strategies to ensure adherence to data protection regulations. These include:

- conducting regular audits to assess data handling practices,
- implementing robust data retention policies aligned with legal frameworks, and
- ensuring staff training to raise awareness of data protection obligations.

Additionally, she emphasized the importance of developing clear policies for data access control, securing sensitive information, and fostering transparency in organizational processes. She posited that by aligning operations with the DPA, promoting accountability, and maintaining a culture of compliance, organizations can safeguard personal data and mitigate risks effectively: She went on to urge participants to undertake the following actions in their organisation to promote compliance with the DPA.

i.Conduct Data Audits and Risk Assessments

Organizations were advised to regularly conducting data audits to track the lifecycle of personal data and identifying potential risks. She submitted that risk assessments should guide the implementation of security measures to prevent breaches.

ii.Develop and Implement Policy Development and Training

She stressed the importance of developing and enforcing comprehensive policies that align with the DPA. She said this could be achieved by implementing training programs across all departments to ensure employees are aware of their responsibilities and best practices for data protection.

iii.Cross-Departmental Collaboration

She advised that departments should be encouraged to work together to achieve compliance. For instance, the IT department's cybersecurity measures should complement the Legal Services department's policy drafting efforts.

iv. Stakeholder Engagement

She further promoted engagement with external stakeholders, including suppliers and service providers, to ensure they align with the organization's data protection standards.

v.Monitoring and Continuous Improvement

She also implored organizations to establish mechanisms for monitoring compliance and addressing gaps. She recommended to organizations to use feedback from audits and assessments to refine policies and procedures continuously.

vi. Key Policies for Compliance

She outlined the following policies as fundamental to compliance with the DPA and encouraged entities to ensure that they have these policies in place as a bare minimum.

- *Data Protection Policy*
- *Staff Data Protection Policy*
- *Data Privacy Policy*
- *Cybersecurity Policy with Incidence Response Plan*
- *IT Policy*
- *Data Transfer Agreement*
- *Compliance Policy*
- *Data Sharing Agreement*

Ms George concluded by observing that the Botswana Data Protection Act (DPA) presents both challenges and opportunities for organizations. She highlighted that by clearly defining departmental roles and adopting proactive compliance strategies, organizations can meet legal obligations while also building trust, enhancing their reputation, and driving sustainable growth.

Ms. George stressed that each department plays a crucial role in safeguarding personal data and ensuring adherence to the highest standards of transparency, confidentiality, and integrity. She reiterated that compliance is not just a legal necessity but a cornerstone of modern business sustainability. With robust data protection measures in place, organizations in Botswana can navigate the evolving digital landscape confidently while safeguarding the interests of all stakeholders.

"Delegates in attendance"


11:00

Presentation 2

Evolution of Data Protection Laws- Global Context:

By: Mr Kgotso Botlhole (*Managing Partner Botlhole Law Group***)**

Presenter- ***Mr Kgotso Botlhole***

In his presentation, Mr. Kgotso Botlhole outlines how data privacy and protection laws have evolved over the years, adapting to the changing demands of global societies and economies. The presentation traces the key milestones in this transformation, with a particular focus on Africa's unique perspective on data privacy. It also highlights the regional frameworks that have emerged, emphasizing Botswana's own data protection framework. Mr. Botlhole argues for a paradigm shift, advocating for the view that data protection should be seen not just as a legal requirement but as a vital enabler for economic growth.

The evolution of data privacy and protection laws has seen significant global strides, with several key milestones shaping the legal landscape over time. The focus of the report is on the global journey, Africa's regional developments, and Botswana's approach, highlighting the economic potential of data protection laws, especially the Data Protection Act of 2018.

1. Global Timeline of Data Privacy and Protection Laws

The inception of comprehensive data protection laws can be traced back to 1981 with the adoption of the Data Protection Convention Treaty 108 by the Council of Europe. This Treaty marked the formal recognition of privacy as a legal right rather than a conceptual one. The European Union (EU) took a major step forward in 1995 with the European Data Protection Directive, designed to regulate personal data processing within the region. However, rapid technological changes and globalization led to the introduction of the General Data Protection Regulation (GDPR), which was finalized in 2016 and enforced in May 2018. The GDPR has since become the gold standard for data privacy,influencing legislation across the globe, including Africa.

2. Africa's Approach to Data Privacy and Protection

Africa's progress in data privacy has been shaped by its distinct socio-political and economic contexts. While the 1981 African Charter on Human and Peoples' Rights did not specifically address privacy, the 1990 African Charter on the Rights and Welfare of the Child recognized the right to privacy. A more comprehensive legal approach came with the 2014 Malabo Convention, a binding treaty by the African Union (AU) covering personal data protection, cybersecurity, and electronic transactions. The treaty has been adopted by 15 member states, including Angola, Gabon, Senegal, and Zambia.

3. Sub-Regional Frameworks for Data Privacy in Africa

Several African sub-regional groups have made strides in developing data protection frameworks:

i. SADC Model Law on Data Protection (2012): This law, influenced by European models, guides the Southern African Development Community (SADC) but remains non-binding, limiting its direct effect on national reforms.

ii. ECOWAS Supplementary Act on Data Protection (2010): ECOWAS, the first sub-regional bloc to adopt a concrete data protection legal framework, set the groundwork for the Malabo Convention.

iii. East African Community (EAC) Framework: While the EAC has a cyber law, it has not yet established a comprehensive personal data protection framework, leaving gaps in regional harmonization.

4. Botswana's Data Privacy and Protection Framework

Botswana's commitment to data privacy dates to 1966, with Section 9 of the Constitution recognizing the right to privacy. This laid the foundation for the country's subsequent data protection legislation. The Data Protection Act of 2018, modelled on the GDPR, represents a significant milestone in aligning Botswana with global data protection standards. It provides rights and obligations that ensure Botswana's participation in the global digital economy.

5. The Paradigm Shift: Data Protection as an Economic Tool

Data protection is increasingly being seen not just as a compliance issue but as an economic driver. The Data Protection Act therefore provides several economic opportunities such as:

i.Data Localization: The requirement for data localization necessitates local infrastructure investments, stimulating job creation and growth in technology industries.

ii.Impact Assessments: The mandated data protection impact assessments (DPIAs) create opportunities for local consultancy services, fostering a sustainable industry in data governance.

iii.Digital Economy: With secure and ethical data handling, Botswana can establish itself as a trustworthy participant in the global digital economy, potentially attracting foreign direct investment and fostering technological innovation.

Mr Botlhole further posited that the evolution of data privacy laws highlights the critical importance of privacy in the digital age. He noted that, in the context of Botswana, the Data Protection Act should be viewed not just as a tool for regulatory compliance but as a strategic asset for driving economic development. He explained that the Act has the potential to foster a culture of data security, stimulate growth in local industries, and position Botswana as a trusted partner in the digital economy. He noted that it is essential to shift the perception of data protection from being a regulatory burden to recognizing it as a cornerstone for sustainable economic growth.

He further outlined several key takeaways and learning points regarding data privacy laws. He highlighted the global evolution of privacy regulations, tracing their foundation to the Data Protection Convention of 1981, followed by the EU Data Protection Directive in 1995, and culminating in the GDPR, which became the global standard in 2018.

From an African perspective, he emphasized the significance of the African Union's Malabo Convention, adopted in 2014, as a foundational framework for personal data protection and cybersecurity across the continent. He also noted regional efforts in Africa, mentioning that sub-regional bodies like SADC, ECOWAS, and the EAC have made strides in developing data privacy frameworks, although gaps persist in some areas.

Focusing on Botswana's framework, Mr. Botlhole observed that the country's constitutional recognition of privacy in 1966 and the introduction of the Data Protection Act in 2018 reflect alignment with global best practices, which positions Botswana for success in the digital economy. Finally, he emphasized a necessary paradigm shift, advocating for the Data Protection Act to be viewed as an economic enabler capable of driving job creation, technological advancement, and foreign investment in Botswana.

Mr Botlhole proposed several action points as part of his policy recommendations. He emphasized the need to promote data localization by developing policies that encourage investments in local data infrastructure, thereby fostering a robust data governance ecosystem. He also highlighted the importance of capacity building, calling for the training of professionals in areas such as data protection impact assessments and other compliance measures to strengthen local expertise. Additionally, he advocated for enhanced regional integration, urging collaboration with other African nations to harmonize data protection laws, which would support economic and technological integration across the continent.

He went on to outline a strategic focus to maximize the benefits of the Data Protection Act. He suggested positioning Botswana as a digital hub by leveraging the Act to establish the country as a secure and attractive destination for global technology investments. He also emphasized the importance of public awareness campaigns to educate businesses and individuals on the Act's potential to drive economic and technological growth. Furthermore, he recommended the implementation of monitoring and evaluation mechanisms to assess the Act's impact, including metrics such as *job creation, investment inflows, and technological innovation.*

Mr Botlhole emphasized the importance of engaging the private sector to maximize the potential of the Data Protection Act. He recommended collaboration with businesses to identify industries that could significantly benefit from the Act's implementation. Additionally, he suggested incentivizing compliance by offering tax incentives or grants to companies that invest in local data infrastructure and adhere to the Act's requirements.

The presentation highlighted the transformative potential of data protection laws, with a particular focus on Botswana's Data Protection Act. It emphasized that by adopting a forward-looking approach, stakeholders could leverage the Act to drive economic development, promote regional collaboration, and position Botswana as a leader in data governance and technological innovation. The presentation underscored that aligning policies, building local capacity, and engaging stakeholders would be essential in shifting data protection from a mere compliance requirement to a cornerstone of economic growth.

Presentation 3

Data Protection Through the Lens of Judicial Decisions:

Ms Senwelo Modise (*Partner at Bookbinder Business Law***)**

Presenter- ***Ms Senwelo Modise***

This presentation provides a detailed summary of key case law and statutory provisions relating to data subjects' rights, legitimate interests in data processing, adequacy decisions for international transfers, and the independence of Data Protection Officers (DPOs), as defined under international and local frameworks. Ms Modise noted that even though there is no case law in Botswana relating to the Data Protection Act, it was important to make reference to case law from other regions to learn from their experience particularly that the DPA is tailored along the GDPR.

1. Right to Access Personal Data

Ms. Senwelo Modise explained that Section 42 of the Data Protection Act (DPA) grants data subjects the right to access their personal information. She referred to two significant cases under the GDPR that have clarified the scope of this right:

a). J.M. v. Pankki S (Case C-579/21): This case highlighted the tension between the right of data subjects to access their data and the privacy rights of third parties. In this case, J.M., a former employee and customer of a Finnish bank, requested access to records from 2013, including the identities of staff who accessed the data, access dates, purposes, and log data. The bank denied the request, citing staff privacy rights and the lawful nature of the access.

Ms. Modise noted that in this case the Court ruled access requests submitted after the GDPR's enforcement date could include data processed before its implementation.

b). RW v. Österreichische Post AG (Case C-154/21): Significantly the CJEU found that subject are entitled to obtain either:

a). Information about the specific recipients to whom their personal data have been or will be disclosed or

b). information about the categories of the recipent. The information provided to the data subject pursuant to the right of access contained in Article 15(1)© must be as precise as possible to enableto enable the data subject to effectively exercise his or her rights under the GDPR.

The court further held that the right of access may be restricted in certain circumstances where it

is impossible to disclose the identity of the specific recipients, such as where those specific recipients are not yet known.

Ms. Modise explained that in this case, the CJEU emphasized data subjects' right to receive detailed information about either specific recipient of their data, where known, or categories of recipients if specific identities were unavailable. She said that this suggested that the information provided must be detailed enough to allow the data subject to exercise their GDPR rights. She also noted that, however, the court acknowledged that limitations could apply where the identities of recipients cannot be reasonably ascertained.

She observed that in both cases, the rulings illustrate the balance required between ensuring data subjects' access rights and respecting the privacy rights of others involved in the data processing chain.

2. Legitimate Interests in Data Processing

Ms. Modise discussed the concept of legitimate interests in data processing, as outlined in Section 26(f) of the Data Protection Act (DPA). She explained that the DPA permits data processing based on legitimate interests, provided these are balanced against the fundamental rights of the data subject.

She referenced the case of **Royal Dutch Lawn Tennis Association (KNLTB) v. Dutch Data Protection Authority (C-621/22),** where the CJEU ruled that a commercial interest could qualify as a legitimate interest under GDPR, provided the processing aligns with other regulatory provisions. She highlighted that the Court stressed the need for a case-by-case assessment to weigh the controller's interests against the data subject's rights and freedoms. This ensures that the legitimate interest clause is not misused as an unrestricted justification for data processing. She underscored the importance of maintaining this balance to uphold both organizational needs and the protection of individual rights.

3. Adequacy Decisions and International Data Transfers

Ms Modise elaborated on adequacy decisions and international data transfers, as governed by Section 75 of the Data Protection Act (DPA). She explained that this section mandates that personal data transfers to third countries are permissible only if those countries provide adequate data protection standards.

She referenced the case of **The Incorporated Trustees of Ikigai Innovation Institute v. National Information Technology Development Agency,** decided by the Federal High Court of Abuja in November 2023. The Court invalidated Nigeria's approval for data transfers to Guinea-Bissau, Sierra Leone, and Comoros, citing their lack of data protection laws or independent authorities. Ms. Modise pointed out that this ruling underscore the necessity of rigorous evaluations when determining adequacy decisions to ensure compliance with global data protection standards.

She posited that robust scrutiny of adequacy assessments is critical for maintaining trust and upholding international data protection frameworks.

4. Independence of Data Protection Officers (DPOs)

Ms Modise went on to discuss the independence of Data Protection Officers (DPOs), as mandated by Section 71 of the Data Protection Act (DPA). She explained that the DPA requires DPOs to operate independently and without conflicts of interest to maintain the integrity of data protection efforts.

She referred to ZS v. Zweckverband 'Kommunale Informationsverarbeitung Sachsen' ("KISA"), C-560/21, where the dismissal of ZS as a DPO due to alleged conflicts of interest brought attention to this requirement. The CJEU ruled that DPOs, whether internal employees or external consultants, must perform their duties

autonomously and remain free from influence by employers or other conflicting roles.

Ms. Modise also **highlighted the case of X-FAB Dresden GmbH & Co. KG**, which reaffirmed that DPOs must avoid professional activities that could conflict with their responsibilities. She stressed that maintaining the independence of DPOs ensures unbiased oversight of data protection practices and the effective safeguarding of data subjects' rights.

In her conclusion, Ms. Modise emphasized that the discussed cases and statutory provisions illustrate the dynamic nature of data protection law. She pointed out key themes, such as balancing conflicting rights (e.g., access versus privacy), ensuring adherence to international data transfer standards, and preserving the independence of DPOs as pivotal to sustained data protection compliance. She noted that these principles are crucial for fostering trust, accountability, and the lawful processing of personal data in any organization handling personal data.

"Delegates in attendance"

SESSION 3

- **Panel Discussion 1:**
  The Role of Data Protection in Media & Communication

- **Panel Discussion 2:**
  The Future of Data Protection in the Age of AI and Big Data

- **Panel Discussion 3:**
  Data Protection Compliance in the Digital Banking Age

Panel Discussion 1:

Moderator:
Mr. Fungai Mazarura (*Business & Public Relations Consultant***)**

Panelist
Mr. Spencer Mogapi *(Former Editor: Sunday Standard, Communications Expert)*

Panelist
Mr Igamu Bonyongo *(Corporate Legal Advisor, Kingsway Consultancy)*

Panelist
Mr. Simon Bathusi (*Partner at Armstrongs***)**

Panelist
Ms. Shathani Molefe *(Chief Compliance Officer, Standard Chartered Bank)*

The Role of Data Protection in Media & Communication

Introduction

The panel discussion, led by Mr. Fungai Mazarura, focused on the intricate and evolving role of data protection in media and communication. The discussion drew insights from industry experts with diverse professional backgrounds, offering a comprehensive perspective on the subject.

1. Spencer Mogapi (*Former Editor: Sunday Standard, Communications Expert***)**

Mr Spencer Mogapi kickstarted the panel discussion by highlighting the critical intersection between data protection and journalism. He projected how modern journalism increasingly relies on data analytics and digital platforms for content delivery, and noted that with this shift, comes significant privacy concerns.

Mogapi pointed out that media organizations often collect and store large volumes of personal data, including information on sources, audience behaviour, and subscriptions. He raised the ethical question of "how much data is too much" and the responsibility of journalists to safeguard their sources in the digital age.

Key insight

Mogapi argued for a balanced approach where transparency in data handling becomes an industry norm. He also noted the need for a strong regulatory framework that does not stifle press freedom but ensures accountability. In his view, media houses must invest in cybersecurity and develop internal guidelines for ethical data use.

Debate

He questioned whether journalists' access to private data limits should have restrictions, especially in cases of public interest stories, sparking a debate on balancing investigative reporting with individuals' rights to privacy.

2. Mr. Igamu Bonyongo (*Corporate Legal Advisor, Kingsway Consultancy***)**

Mr. Bonyogo provided a legal perspective to the discussion, focusing on the compliance challenges media and communication entities face under global and local data protection laws, such as the General Data Protection Regulation (GDPR) and Botswana's Data Protection Act.

He outlined the legal obligations of media houses, such as obtaining consent for data collection, maintaining secure systems, and ensuring compliance with cross-border data transfer regulations. Bonyogo highlighted real-world scenarios where media companies faced hefty fines for breaches, emphasizing the financial and reputational risks involved.

Key Insight

He proposed that media companies should establish data protection officers (DPOs) to navigate compliance issues. He also stressed the need for continuous staff training on data privacy laws.

Suggestion

Bonyogo recommended that governments collaborate with media houses to create standardized guidelines that both protect personal data and accommodate the realities of investigative journalism.

3. Simon Bathusi (*Partner at Armstrongs***)**

Simon Bathusi approached the topic from a corporate governance and risk management perspective. He emphasized the importance of embedding data protection practices within the organizational culture of media and communication entities.

He noted that breaches are often the result of inadequate governance, such as poorly defined data handling policies or negligence by employees. Bathusi proposed a risk-based approach to data protection, where companies conduct regular audits, identify vulnerabilities, and implement mitigation strategies.

Key Insight
Bathusi discussed the potential for data breaches to damage public trust in media institutions, making it critical for companies to demonstrate a commitment to ethical practices.

Debate
Bathusi raised the controversial topic of media organizations using consumer data for targeted advertising. He questioned whether this practice aligns with the principles of data protection, sparking a lively debate among the panellists.

4. Shathani Molefe (*Chief Compliance Officer, Standard Chartered Bank*)

Shathani Molefe brought a financial sector perspective to the discussion, drawing parallels between banking and media in terms of the sensitivity of data they handle. She highlighted the importance of robust compliance frameworks and how media organizations could learn from the banking sector's practices.

Molefe stressed the growing prevalence of cybercrime targeting personal data, calling for stronger industry collaboration to address these threats. She suggested that media companies partner with cybersecurity firms to stay ahead of evolving risks.

Key Insight
Molefe emphasized the importance of customer trust, suggesting that transparent data policies and clear communication about how data is used could enhance the credibility of media organizations.

Suggestion
Molefe advocated for integrating data protection into the corporate social responsibility (CSR) initiatives of media companies, positioning themselves as champions of digital rights and privacy.

5. Conclusion by Moderator: Mr. Fungai Mazarura

Mr. Mazarura concluded the session by summarizing the panellists' key points. He noted that while data protection poses significant challenges, it also offers an opportunity for media and communication entities to build trust and differentiate themselves in a competitive landscape.

He highlighted the need for collaborative efforts between media, regulators, and legal experts to create an ecosystem that prioritizes both innovation and privacy while not impeding on the free speech doctrine. The session ended with a consensus that data protection is not just a legal obligation but a moral and strategic imperative in the modern era of media and communication.

Moderator and panelists of Panel Discussion 1 (The Role of Data Protection in Media & Communication)

Panel Discussion 2:

Moderator:
Professor Sizwe Snail (*South African Cyberlaw and AI Law Expert***)**

Panelist
Mr. Tumelo Bethuelson *(Manager, Business Intelligence, FNBB)*

Panelist
Mr. Thabiso Oabile *(Chief Technology Officer, Botswana Insurance Company)*

Panelist
Dr. Bokamoso Basutli (*Senior Lecturer, Department of Electrical, Computer, and Telecommunications Engineering, BIUST, and BOCRA Board Member***)**

The Future of Data Protection in the Age of AI and Big Data

Introduction

The panel discussion, moderated by Professor Sizwe Snail, explored the dynamic intersection of artificial intelligence (AI), big data, and data protection laws, focusing on future challenges, opportunities, and actionable solutions. Below is a summary of the insights, debates, and suggestions shared by each panellist during the session.

1. Mr. Tumelo Bethuelson (Manager, Business Intelligence, FNBB**).**

Mr. Bethuelson emphasized the transformative role of big data in shaping business intelligence and customer personalization. He explained that banks increasingly rely on AI-driven algorithms to analyse customer data for risk assessments, fraud detection, and tailored product offerings. However, he raised concerns about balancing innovation with privacy compliance.

He pointed out that the sheer volume and velocity of big data pose risks of data breaches and misuse if not properly governed. In Botswana's context, he argued that frameworks like the Data Protection Act of 2018 should be adapted to address the complexities introduced by AI, such as the challenge of accountability for decisions made by AI systems.

Mr. Bethuelson proposed that businesses should adopt transparent AI governance models and ensure robust encryption protocols for data security. He also called for financial institutions to educate consumers about how their data is used, building trust and fostering a privacy-conscious culture.

Key Insight

AI and big data offer immense value to businesses, but these technologies must be deployed responsibly, with clear accountability frameworks to address emerging privacy risks.

2. Mr. Thabiso Oabile (Chief Technology Officer, Botswana Insurance Company*)*

Mr. Oabile highlighted the insurance industry's increasing dependence on AI and big data for predictive analytics and decision-making. He noted that machine learning algorithms are now used to assess policyholder risks, streamline claims processes, and detect fraudulent activities.

However, he argued that the ethical implications of AI must not be overlooked. He raised concerns about algorithmic bias, where AI systems might unintentionally discriminate against certain groups due to biased training data. In the context of data protection, he questioned whether existing legal frameworks in Botswana and the SADC region are equipped to address such nuanced issues.

Mr. Oabile proposed three key strategies to address these challenges:

i.Regulatory Modernization: He suggested that policymakers update data protection laws to account for AI-specific challenges, such as algorithmic accountability and the right to explanation.

ii.Collaborative Ecosystems: He called for closer collaboration between regulators, tech companies, and academia to develop ethical AI guidelines tailored to the region.

iii.Continuous Monitoring: He recommended adopting dynamic compliance mechanisms that evolve with the rapid advancements in AI and big data technologies.

Key Insight

The future of data protection will depend on proactive regulation, collaboration, and continuous monitoring to address the ethical and privacy implications of AI in industries like insurance.

3. Dr. Bokamoso Basutli (Senior Lecturer, BIUST,

and BOCRA Board Member)

Dr. Basutli provided a technical perspective on the intersection of AI, big data, and data protection. He argued that AI's reliance on vast datasets for training and optimization raises critical questions about data ownership, consent, and security. He stressed that ensuring data protection in the AI age requires both regulatory interventions and technological innovations.

Drawing from his role at BOCRA, he underscored the importance of developing Botswana-specific solutions, given the unique socio-economic and technological landscape. He recommended that organizations adopt privacy-preserving technologies such as federated learning and differential privacy to minimize risks while leveraging AI capabilities.

Dr. Basutli also raised the issue of cross-border data flows, noting that AI systems often rely on global datasets. He called for regional harmonization of data protection laws to ensure consistent standards across the SADC region. Additionally, he highlighted the need for educational initiatives to build local expertise in AI ethics and data protection.

Key Insight
Botswana must adopt privacy-preserving technologies and foster regional collaboration to address the cross-border challenges posed by AI and big data.

4. Moderator's Reflections: Professor Sizwe Snail

Professor Snail summarized the discussion by emphasizing that the future of data protection in the AI era hinges on balancing innovation with ethical and legal safeguards. He noted that the perspectives shared by the panellists underscored the need for a multi-stakeholder approach to address the challenges and opportunities of AI and big data.

He highlighted three overarching themes from the discussion:

i.Accountability in AI Decision-Making: Policy makers must ensure that data protection laws provide clear guidelines for algorithmic accountability.

ii.Ethical AI Practices: Businesses and regulators should work together to eliminate biases and ensure fairness in AI applications.

iii.Capacity Building: Investment in local expertise and education is critical for developing sustainable AI and data governance ecosystems.

Professor Snail closed the session by encouraging stakeholders to view data protection not as a barrier to innovation but as a foundation for building trust and fostering sustainable technological growth in the region.

The panel discussion underscored the complexity of safeguarding data protection in the age of AI and big data. It highlighted the need for updated regulations, technological innovations, and collaborative efforts to ensure privacy and ethical practices. By addressing these challenges proactively,Botswana can position itself as a leader in data governance and AI innovation in Africa.

Moderator and panelists of Panel Discussion 2: (The Future of Data Protection in the Age of AI and Big Data)

Panel Discussion 3:

Moderator:
Ms. Sedilame Modiga (*Manager, Business Compliance Advisory, Stanbic***)**

Panelist
Ms Lorato Kgosidiile *(Associate Attorney, Botlhole Law Group)*

Panelist
Ms. Kutlwano Tatolo *(Legal Counsel and Board Secretary, Bofinet)*

Panelist
Mr. Petros Molefe (*Chief Information Officer, Standard Chartered Bank***)**

Data Protection Compliance in the Digital Banking Age

Introduction

The panel discussion, moderated by Ms. Sedilame Modiga, delved into the pressing challenges and opportunities associated with ensuring data protection compliance in the rapidly evolving digital banking landscape. Following is a narrative summary of the insights, debates, and suggestions presented by the panellists.

1. Lorato Kgosidiile (Associate Attorney, Botlhole Law Group**)**

Ms. Kgosidiile opened the discussion by outlining the legal and regulatory implications of data protection in the digital banking age. She emphasized the pivotal role of the Data Protection Act of 2018 in Botswana, which aligns with global frameworks such as the GDPR to ensure that personal data is collected, processed, and stored securely and lawfully.

She noted, however, that compliance remains a challenge for many financial institutions, particularly in interpreting complex legal requirements. For example, she pointed out that banks must navigate issues such as obtaining explicit consent, protecting sensitive data, and ensuring secure cross-border data transfers.

Ms. Kgosidiile advocated for greater collaboration between financial institutions and regulators to clarify compliance requirements. She also recommended that banks implement robust privacy policies and employee training programs to mitigate risks of data breaches. Furthermore, she suggested that legal advisors should play a proactive role in helping banks integrate compliance into their digital transformation strategies.

Key Insight
Legal clarity and proactive collaboration with regulators are essential for ensuring effective data protection compliance in digital banking.

2. Ms. Kutlwano Tatolo (Legal Counsel and Board Secretary, Bofinet**)**

Ms. Tatolo approached the topic from the perspective of a telecommunications provider and its intersection with the banking sector. She highlighted how the increasing reliance on digital platforms, particularly mobile banking, has created a complex ecosystem where data protection compliance must extend across multiple stakeholders.

She stressed the importance of implementing data-sharing agreements between banks, telecom providers, and fintech companies to ensure consistent compliance standards. Ms. Tatolo also noted that banks must take steps to safeguard not just their internal systems but also the entire supply chain, particularly when outsourcing data storage and processing to third-party providers.

One of her major concerns was the potential for cybersecurity vulnerabilities in the digital banking ecosystem, where weak links in third-party systems could expose customers' personal and financial data. She urged banks to adopt stringent due diligence protocols when partnering with external service providers and to conduct regular audits to ensure compliance.

Ms. Tatolo also emphasized the need for Botswana to harmonize its data protection laws with regional frameworks, such as the SADC Model Law, to address the challenges posed by cross-border transactions.

Key Insight
Ensuring compliance in digital banking requires robust partnerships, secure supply chains, and regional harmonization of data protection laws.

3. Mr. Petros Molefe (Chief Information Officer, Standard Chartered Bank**)**

Mr. Molefe provided a technological perspective to the discussion, focusing on how digital transformation in banking has heightened

the need for innovative compliance solutions. He noted that while digital banking offers unparalleled convenience and accessibility, it also increases the risks of cyberattacks, data breaches, and fraud.

To address these challenges, he recommended that banks invest in advanced technologies such as encryption, multi-factor authentication, and real-time fraud detection systems. He argued that adopting AI-driven compliance tools could help banks monitor and detect potential breaches more effectively.

Mr. Molefe also discussed the importance of customer education, noting that many data breaches occur due to weak user passwords and phishing attacks. He suggested that banks implement awareness campaigns to help customers understand their role in maintaining data security.

Additionally, he highlighted the growing role of regtech (regulatory technology) in simplifying compliance processes. For instance, automated systems can streamline tasks such as reporting, data audits, and risk assessments, reducing the burden on compliance teams while ensuring accuracy.

Key Insight
Leveraging advanced technologies and customer education are critical to maintaining compliance and safeguarding data in digital banking.

4. Moderator's Reflections: Ms. Sedilame Modiga

Ms. Modiga summarized the discussion by highlighting the multifaceted nature of data protection compliance in digital banking. She noted that the panellists collectively underscored the need for legal, organizational, and technological solutions to address emerging risks and challenges.

She emphasized three key themes:

i.Legal and Regulatory Alignment: Clear and practical regulations are necessary to guide compliance in the digital age.

ii.Stakeholder Collaboration: Banks, telecoms, and fintechs must work together to ensure consistent compliance standards.

iii.Technology and Innovation: Advanced tools and customer education can help mitigate risks and improve data protection.

Ms. Modiga called for ongoing dialogue among regulators, financial institutions, and technology providers to create a secure and compliant digital banking environment that fosters trust and innovation.

The panel discussion highlighted that data protection compliance in the digital banking age is both a challenge and an opportunity. By adopting a collaborative, technology-driven, and proactive approach, Botswana's banking sector will not only comply with data protection laws but also enhance customer trust and drive digital innovation. Stakeholders were urged to view compliance as a strategic asset rather than a regulatory burden, ensuring that digital banking continues to thrive in a secure and compliant manner.

Panel Discussion 3: Data Protection Compliance in the Digital Banking Age

DAY 2 PROCEEDINGS:

SESSION 4

- **Presentation 4**
  Implementation of Data Protection Laws in Ghana, Implementation & Enforcement as the First Data Protection Commissioner – Strides Made:

- **Presentation 5**
  GDPR as International Best Practice

6TH DECEMBER 2024

Presentation 4

Implementation of Data Protection Laws in Ghana, Implementation & Enforcement as the First Data Protection Commissioner – Strides Made:

By: Dr Quintin Akrobotu (*Director, Regulatory & Compliance***)**

In his presentation, Quintin Akrobotu, the first Data Protection Commissioner of Ghana, shared insights into the journey of implementing data protection laws in the country, highlighting the strides made,challenges faced, and the path ahead. Ghana was one of the first countries in Africa to enact a Data Protection Act (2012), and Akrobotu's discussion provided an in-depth look into the practicalities of implementing and enforcing these laws in a rapidly evolving digital landscape.

1. Implementation of Data Protection Laws in Ghana

Akrobotu began his presentation by acknowledging the significance of Ghana's early adoption of data protection laws in 2012. As the first Data Protection Commissioner in Ghana, he explained the pivotal role the Data Protection Commission (DPC) played in shaping and guiding the implementation of these laws.

i.The Role of the Data Protection Commission: The DPC was tasked with enforcing data protection principles, monitoring data processing practices, and ensuring that individuals' privacy rights were upheld. Akrobotu emphasized the importance of establishing clear regulatory frameworks for businesses, governmental bodies, and individuals to follow, as it helped build public trust and compliance.

ii.Public and Private Sector Collaboration: He highlighted the necessity of collaboration between the public and private sectors in ensuring the effective implementation of data protection laws. The DPC worked closely with organizations, providing training and awareness campaigns to assist businesses in aligning their operations with the Data Protection Act. He noted that such partnerships were crucial in ensuring that data protection measures were understood and adhered to across different industries.

Key Achievements

Akrobotu cited several key achievements in the implementation process:

i. The establishment of a national registry for data controllers and processors.

ii. Increased awareness among citizens and businesses regarding their data rights and obligations.

iii. Successful investigations and penalties imposed on organizations failing to comply with the laws.

iv.The development of a Data Protection Trust Fund, which was used to support enforcement activities and training programs

2. Challenges in Implementation and Enforcement

Despite the successes, the presentation also delved into the significant challenges Ghana faced in the implementation and enforcement of data protection laws:

i. Lack of Awareness and Understanding: One of the primary obstacles was the lack of awareness among both businesses and the general public about the importance of data protection. Many individuals were not fully aware of their privacy rights, and businesses struggled with how to implement effective data protection measures. Akrobotu noted that education and awareness were ongoing challenges that required constant effort.

ii. Capacity Constraints: The DPC faced limitations in terms of financial and human resources, which hindered its ability to monitor compliance and enforce the law comprehensively. While the regulatory framework was in place, Akrobotu stressed that effective enforcement requires sufficient personnel, technological tools, and funding to ensure that violations were identified and penalized in a timely manner.

iii. Technological Advancements: With the rapid growth of digital technologies, the DPC had to keep up with new developments such as cloud computing, artificial intelligence (AI), and big data. These technologies presented complex challenges in terms of how personal data was being processed, stored, and shared. Akrobotu highlighted the need for continuous updates to the regulatory framework to address emerging technologies.

iv.Cross-border Data Transfers: Ghana faced challenges with cross-border data flows, especially in the context of international data sharing. Ensuring that personal data was handled securely across borders and in line with Ghana's legal framework posed difficulties, especially when companies outsourced or worked with international partners. Akrobotu emphasized the need for international cooperation and harmonization of data protection laws across African countries to address these issues.

3. Debate and Discussion

The presentation sparked a lively debate among the attendees regarding the broader implications of data protection enforcement in Ghana and across Africa.

i. Need for Stronger Penalties: Some panellists suggested that although Ghana had made strides, penalties for non-compliance were still not sufficiently strong to deter violations. Akrobotu responded by acknowledging that while penalties were in place, enforcement capacity and the need for more robust regulations were key areas of focus moving forward.

ii. Adapting to Technological Changes: There was a discussion about how technological advancements, especially in AI and big data, were outpacing data protection laws. Akrobotu agreed, stating that the DPC needed to be proactive in revising policies and collaborating with tech industry leaders to understand the implications of these technologies on data privacy.

iii.Collaboration and Capacity Building: A recurring theme in the discussion was the importance of collaborative efforts and capacity building in the implementation of data protection laws. Participants stressed the need for a multi-stakeholder approach involving government, private sector, and civil society organizations to build a culture of data protection across the country. Akrobotu emphasized that this approach had been crucial in Ghana's success and was something that would continue to be a focus.

iv.The Role of Public Awareness: There was a consensus that improving public awareness was essential to the success of data protection laws. Akrobotu mentioned that ongoing efforts were being made to educate citizens about their data rights, but there was a need for targeted campaigns to address different segments of society, especially vulnerable groups.

4. Suggestions and Insights

Akrobotu concluded his presentation by offering several suggestions and insights on the way forward for data protection in Ghana and beyond:

i.Continuous Training and Capacity Building: Regular training programs for both regulatory authorities and businesses were vital. This would help ensure that everyone involved in the processing and handling of personal data was up to date with the latest developments and regulatory requirements.

ii.Leveraging Technology for Compliance: Akrobotu encouraged businesses to adopt data protection technologies that can automate compliance processes, monitor data usage, and

protect sensitive information. Regulatory bodies could also benefit from using technology to enhance their enforcement capabilities, such as utilizing AI-powered tools for identifying violations.

iii.Strengthening Data Protection Laws: While the current framework in Ghana was a strong foundation, Akrobotu called for continued legislative reforms to keep up with rapidly evolving technologies and global best practices. This would include enhancing regulations around cross-border data transfers and AI applications.

iv.Regional Cooperation: On the international stage, Akrobotu emphasized the importance of regional cooperation among African countries to ensure harmonization of data protection laws. He suggested that data protection commissioners across Africa could work together to establish a unified regulatory approach that could facilitate cross-border data flows while ensuring privacy rights were respected.

v.Private Sector Engagement: Finally, Akrobotu urged the private sector to take a proactive role in implementing data protection measures and to view data protection as an opportunity to build consumer trust rather than a regulatory burden. He also highlighted that businesses should not only focus on compliance but should make efforts to develop a data protection culture within their organizations.

Quintin Akrobotu's presentation provided a valuable and detailed perspective on the implementation and enforcement of data protection laws in Ghana. While the country has made significant strides, the journey is ongoing, with continuous efforts required to tackle challenges such as awareness, resource constraints, technological advancements, and international cooperation. The insights shared during the session were crucial for understanding both the successes and challenges that come with establishing a robust data protection framework, and the discussions raised important considerations for other countries in Africalooking to implement similar laws.

"Delegates in attendance"

Presentation 5

GDPR as International Best Practice

By: Mr. Paul Esselaar (*South Africa Admitted Attorney, Data Protection / Privacy Law, Researcher in ICT Solutions***)**

Presenter- ***Mr. Paul Esselaar***

In his presentation, Mr. Paul Esselaar, a South African admitted attorney with expertise in data protection and privacy law, explored the DPA against General Data Protection Regulation (GDPR) as an example of international best practice in data protection. Esselaar, who has worked extensively in the field of ICT solutions and privacy law, provided a comprehensive overview of how the GDPR has shaped global data protection frameworks and why it serves as a model for other jurisdictions..

Esselaar began his presentation by explaining the GDPR's significance as a pioneering regulation in the field of data protection. Enacted by the European Union in 2018, the GDPR introduced comprehensive rules on how personal data should be handled, focusing on individuals' rights, accountability, and transparency. He argued that the GDPR has not only become a gold standard but also a benchmark that countries around the world are looking to adopt or adapt their laws to.

i.Comprehensive Framework: Esselaar highlighted that the GDPR was the first regulatory framework to provide a comprehensive set of guidelines for data controllers, processors, and users, ensuring that personal data is handled with the utmost care and in compliance with privacy principles. He described the regulation's scope, which covers the collection, processing, storage, and transfer of personal data and ensures that these activities are done in a lawful, transparent, and secure manner.

ii. Focus on User Rights: One of the key pillars of the GDPR, Esselaar explained, is its emphasis on empowering individuals to take control of their personal data. This includes ensuring that users have the right to access their data, the right to request data erasure (the "right to be forgotten"), and the right to correct inaccuracies. According to Esselaar, these rights have set the stage for more user-centric data protection approaches globally.

iii. Accountability and Enforcement: Esselaar pointed out that the GDPR's most significant departure from previous data protection regulations is its focus on accountability. It requires organizations to not only comply with the rules but also demonstrate compliance through documentation, data protection officers (DPOs), and data protection impact assessments (DPIAs). Additionally, the GDPR's enforcement mechanism, with severe penalties for non-compliance (up to 4% of annual global turnover or €20 million, whichever is greater), has set a global precedent for how data protection regulations should be enforced.

1. Debate and Discussion: GDPR as a Global Model

Following the presentation, there was a lively discussion around the global applicability and challenges of adopting the GDPR as a model for data protection in different jurisdictions.

i.Global Influence and Adoption: A significant part of the debate focused on how the GDPR has influenced data protection laws worldwide. Many attendees shared those countries such as Brazil (with its LGPD), South Africa (with the POPIA), and Japan had adopted frameworks like the GDPR.

Esselaar discussed how the GDPR's extraterritorial reach (applying to any organization that processes the data of EU residents) has encouraged non-EU countries to align their laws with its provisions to facilitate international trade and data exchanges.

Some panellists argued that while adopting the GDPR model could help countries streamline their data protection frameworks, there were varying economic and political incentives for compliance. For example, countries looking to boost their digital economy or cloud services industry would benefit from aligning with the GDPR to ensure data adequacy when transferring data to the EU. Esselaar agreed but warned that the GDPR's rigorous requirements could place significant burdens on smaller businesses in developing countries, which may not have the resources for such extensive compliance efforts.

One of the key challenges discussed was how the GDPR's enforcement mechanisms could be difficult to implement in countries with less developed legal and technological infrastructures. Developing countries, in particular, might face difficulties in funding and training the necessary regulatory bodies to monitor compliance. Esselaar acknowledged that this was a valid concern, but he emphasized that countries should not shy away from adapting GDPR principles to their unique contexts, especially as cross-border data flows become more critical.

Another point of contention was the cultural and regional differences in attitudes toward privacy and data protection. Some panellists argued that privacy expectations vary significantly across cultures. For instance, some regions might be more accepting of data processing for commercial purposes, while others might have stringent expectations for data privacy.

Esselaar agreed with this concern and noted that the GDPR is not a one-size-fits-all solution. He suggested that countries and regions should tailor the principles of the GDPR to their specific cultural, legal, and economic environments. He used the example of Africa, where privacy laws are still evolving, but regional cooperation could help align privacy standards across the continent without imposing a one-size-fits-all approach.

2. Suggestions and Insights

Esselaar concluded the presentation with several suggestions on how countries could move forward in adopting and adapting the GDPR model:

i.Gradual Implementation: Esselaar recommended that countries looking to adopt GDPR-like regulations should start with a phased approach. This could involve beginning with simpler data protection measures, building a solid foundation, and gradually incorporating more complex compliance requirements as the country's regulatory infrastructure matures.

ii.Collaboration with Industry: He stressed the importance of collaboration with industry stakeholders to ensure that data protection laws do not stifle innovation. Countries should engage with technology companies, startups, and businesses to ensure that data protection regulations are practical and do not create undue barriers to growth.

iii.Training and Education: Esselaar called for investment in training both for regulators

and businesses. He suggested that there should be greater emphasis on data protection literacy, not just among legal professionals but also within organizations. This would help businesses develop internal compliance mechanisms and ensure that their staff are aware of data protection responsibilities.

iv.International Harmonization: Finally, Esselaar recommended greater international cooperation to harmonize data protection regulations. He pointed out that the global nature of the internet means that data privacy issues are often cross-border in nature. Thus, international standards for data protection could help avoid conflicting regulations and promote smoother data exchanges between countries.

Mr. Paul Esselaar's presentation underscored the significance of the GDPR as international best practice in data protection law. While the GDPR has set a high standard, its adoption globally will require careful adaptation to local contexts and collaborative efforts among countries. The discussion highlighted the challenges that smaller or developing countries may face in implementing and enforcing GDPR-like regulations, but it also pointed out the tremendous benefits of aligning with global data protection standards to foster trust, security, and economic growth in the digital age. The insights provided by Esselaar were invaluable for understanding the broader implications of global data privacy and how nations can take practical steps toward data protection compliance.

"Delegates in attendance"

SESSION 5

- **Panel Discussion 4:**
  Cybersecurity Law, Technology Law

- **Breakaway Session 1:**
  Leveraging Technology to Ensure Compliance and Implementation of Data Protection

- **Breakaway Session 2:**
  Compliance Readiness Checklist

Panel Discussion 4:

Moderator:
Professor Sizwe Snail (*South Africa Cyberlaw and AI Law Expert***)**

Panelist
Ms. Segametsi Mafa (*Managing Director, Service Xcellence, IT & Corporate Governance; \Board Member, BSE***)**

Panelist
Mr. Martin Kamethu *(Head of Operations, Serianu Limited, Botswana Office)*

Panelist
Mr. Pako Phatsimo (*Technology Risk and Governance Manager, FNBB)*

Cybersecurity Law, Technology Law

Introduction

Under the guidance of Professor Sizwe Snail, the panel delved into the intricate and evolving fields of cybersecurity law and technology law. The discussion explored their relevance in the modern technological landscape, challenges faced in implementation, and potential pathways for improvement in Botswana and beyond. Following is a narrative summary of the insights shared by each panellist.

1. Mr. Martin Kamethu (Head of Operations, Serianu Limited, Botswana Office)

Mr. Kamethu approached the topic from an operational and corporate perspective, highlighting the challenges that businesses face in navigating the intersection of technology and law. He pointed out that many organizations in Botswana struggle with compliance due to a lack of understanding of regulatory requirements and limited resources to implement robust cybersecurity measures.

He underscored the need for a risk-based approach to cybersecurity, where laws are tailored to address specific threats and vulnerabilities faced by businesses. Mr. Kamethu also emphasized the importance of cybersecurity audits and assessments in ensuring compliance and mitigating risks.

Additionally, he raised concerns about the slow pace of legislative adaptation to emerging technologies such as artificial intelligence, blockchain, and the Internet of Things (IoT). He argued that existing laws often lag technological advancements, creating a gap that cybercriminals exploit.

To address these challenges, Mr. Kamethu proposed that regulators adopt a proactive legislative framework that anticipates technological changes and incorporates input from industry experts during the drafting process.

Key Insight

Businesses need clearer regulatory guidance and proactive laws to effectively manage technology risks and ensure compliance.

2. Ms. Segametsi Mafa (Managing Director, Service Xcellence, IT & Corporate Governance; Board Member, BSE**)**

Ms. Mafa highlighted the importance of governance in the successful implementation of cybersecurity and technology laws. She stressed that compliance should not be viewed merely as a regulatory requirement but as a critical component of organizational strategy and corporate governance.

She noted that the Botswana Stock Exchange (BSE) has a vested interest in promoting robust governance practices among listed companies, particularly as cyber risks pose significant threats to investor confidence. Ms. Mafa argued that boards of directors must prioritize cybersecurity by embedding it into their governance frameworks and ensuring accountability at the highest levels.

One of her key suggestions was the introduction of mandatory reporting requirements for cyber incidents, which would encourage greater transparency and improve the overall security posture of the corporate sector. She also advocated for regular training and awareness programs to equip executives and employees with the knowledge needed to navigate complex cybersecurity and technology regulations.

Key Insight

Governance is a cornerstone of effective cybersecurity compliance, and boards must lead the charge in integrating cybersecurity into corporate strategy.

3. Mr. Pako Phatsimo (Technology Risk and Governance Manager, FNBB)

Mr. Phatsimo provided a financial sector

perspective, focusing on the interplay between technology risk, governance, and regulatory compliance. He noted that the banking sector is particularly vulnerable to cyber threats due to its reliance on digital platforms and the high value of the data it handles.

He emphasized the importance of aligning cybersecurity laws with international standards such as ISO 27001 and PCI DSS to ensure that Botswana's legal framework is both comprehensive and globally relevant. However, he cautioned that adopting international standards must be accompanied by localized implementation strategies to address Botswana's unique technological and economic landscape.

Mr. Phatsimo also discussed the role of regtech (regulatory technology) in streamlining compliance processes. He highlighted how banks are leveraging AI-driven tools to automate tasks such as monitoring, reporting, and risk assessments, thus reducing the burden on compliance teams.

To strengthen cybersecurity resilience, he called for enhanced public-private partnerships, where the government collaborates with financial institutions to share threat intelligence and develop collective defence mechanisms.

Key Insight
The financial sector must adopt global standards and innovative technologies while fostering public-private collaboration to address cybersecurity risks effectively.

4. Moderator's Reflections: Professor Sizwe Snail

Professor Snail summarized the discussion by acknowledging the diverse perspectives offered by the panellists. He noted that while significant progress has been made in cybersecurity and technology law, gaps remain in implementation, enforcement, and alignment with emerging technologies.

He highlighted three key themes:

i.Dynamic Legal Frameworks: Cybersecurity and technology laws must evolve to keep pace with technological advancements.

ii.Collaborative Governance: Effective compliance requires the active participation of all stakeholders, including government, private sector, and academia.

iii.Capacity Building: Ongoing training and awareness programs are essential for equipping individuals and organizations with the skills needed to navigate complex regulations.

Professor Snail concluded by calling for a unified approach to cybersecurity and technology governance, emphasizing that strong laws alone are insufficient without robust enforcement and stakeholder engagement.

The panel discussion underscored the critical importance of cybersecurity and technology law in safeguarding Botswana's digital ecosystem. Through collaborative efforts, proactive legislation, and a commitment to capacity building, the country can address existing challenges and position itself as a regional leader in cybersecurity governance. The panellists collectively emphasized that success in this domain hinges on the alignment of legal, technical, and organizational strategies, with a shared vision for a secure and innovative digital future.

Breakaway Session 1

Leveraging Technology to Ensure Compliance and Implementation of Data Protection

By: Mr. Fred Webb (*Compliance Lead, Debswana***)**

In this session, Mr. Fred Webb explored the crucial role of technology in enabling the effective compliance and implementation of data protection laws, particularly in the context of Botswana's evolving data privacy landscape. The session aimed to facilitate a discussion on how technology can streamline compliance processes, mitigate risks, and enhance the enforcement of data protection measures.

1. Key Themes and Insights

Mr. Webb began by acknowledging the growing complexity of data protection compliance, especially considering rapid technological advancements. He emphasized that traditional methods of managing data protection and compliance were becoming increasingly inadequate in addressing the challenges posed by digital transformation, big data, and cloud computing.

He highlighted that the implementation of technology-driven compliance systems is no longer optional but necessary for organizations to stay ahead of regulatory requirements, mitigate risks, and protect customer data effectively.

2. The Role of Automation in Compliance

Mr. Webb opened the conversation by discussing the potential of automation in ensuring compliance. He argued that the manual management of data protection obligations—such as tracking consent, data subject requests, and audits—was resource-intensive and prone to human error. Automation, he suggested, offers significant benefits in improving the efficiency and accuracy of these processes.

Key Insight

Automation tools can streamline data protection workflows by ensuring timely responses to data subject requests, tracking consent and processing activities, and reducing the risk of human error. Additionally, it can assist in maintaining detailed records of compliance activities, which is crucial for demonstrating accountability.

3. Use of Artificial Intelligence (AI) in Risk Detection

The discussion then shifted to the role of artificial intelligence (AI) in identifying risks related to data privacy. Mr. Webb noted that AI tools could be leveraged to monitor and detect potential data breaches or non-compliance in real-time. AI can help organizations swiftly address vulnerabilities before they become critical issues.

He highlighted that AI could also be employed in data protection impact assessments (DPIAs) to predict the risks associated with new data processing activities and technologies. AI could assist in identifying areas of concern, enabling companies to address potential compliance issues proactively rather than reactively.

Key Insight

AI-powered tools offer organizations the ability to perform continuous risk monitoring and detection, allowing for real-time intervention and more effective data protection measures.

4. Data Encryption and Blockchain Technology

Mr. Webb then delved into the technical aspects of data security, focusing on data encryption and blockchain technology as tools for ensuring data protection. He explained that encryption provides an additional layer of security for personal data, making it significantly harder for unauthorized parties to access sensitive information.

In terms of blockchain, he argued that this emerging technology holds promise in improving transparency and accountability in data

protection. Blockchain's immutable ledger could provide a transparent record of all data processing activities, allowing for easier tracking of data access and modifications. This feature could be particularly useful for compliance audits, as it ensures that data handling processes are transparent, traceable, and immutable.

Key Insight
Encryption and blockchain technology are vital in securing personal data, ensuring integrity, and providing transparent records that can be used for audits and compliance purposes.

5. Compliance Management Software and Data Governance Tools

Mr. Webb also discussed the growing market for compliance management software and data governance tools, which help organizations manage their data protection obligations in a more structured and systematic way. These platforms integrate various compliance requirements, from documentation and reporting to risk management, into a single interface.

He explained that such software provides an efficient way to track compliance deadlines, maintain records of all data processing activities, and manage third-party vendor compliance. By centralizing all data protection activities, organizations can more easily demonstrate compliance with data protection laws and regulations during audits and inspections.

Key Insight
Using specialized compliance management and data governance tools can enhance transparency, simplify the management of compliance activities, and ensure that data protection obligations are consistently met across an organization.

6. Overcoming Implementation Challenges

Despite the benefits of leveraging technology, Mr. Webb acknowledged several challenges that organizations face when implementing these tools. He pointed out that many businesses, particularly smaller ones, lack the resources or technical expertise to deploy complex compliance technologies effectively. Furthermore, the integration of new technologies into existing infrastructures can be costly and time-consuming.

He emphasized the importance of capacity building and continuous education for data protection officers, compliance teams, and IT personnel. This includes keeping up-to-date with the latest tools, regulations, and best practices in the rapidly changing landscape of data privacy and protection.

Key Insight
Effective implementation of technology in data protection requires not only the right tools but also skilled personnel capable of integrating and managing these technologies in a way that maximizes their potential.

7. Regulatory Compliance and Global Standards

The session concluded with a discussion on the global alignment of data protection laws, especially in light of international frameworks like the General Data Protection Regulation (GDPR). Mr. Webb highlighted that many companies operating in Botswana are also bound by international data protection regulations, necessitating compliance with global standards.

He recommended that Botswana-based organizations adopt a multi-jurisdictional compliance strategy to ensure they meet both local and international data protection requirements. This approach would enable businesses to operate seamlessly across borders while maintaining high standards of data privacy and security.

Key Insight
Adopting a global compliance strategy ensures that companies can operate internationally without risking non-

non-compliance with varying data protection regulations.

Mr. Webb concluded the session by emphasizing the necessity of technology in modern data protection compliance. He reiterated that while technological tools can enhance compliance efforts, organizations must ensure they have the proper resources, expertise, and strategies in place to leverage these technologies effectively.

Key Takeaways

i.Technology, including automation, AI, encryption, and blockchain, plays a vital role in ensuring compliance and safeguarding personal data.

ii.Organizations must invest in capacity building and continuous training to effectively implement and manage data protection technologies.

iii.Adopting a multi-jurisdictional compliance strategy ensures alignment with both local and global data protection standards..

"Delegates in attendance"

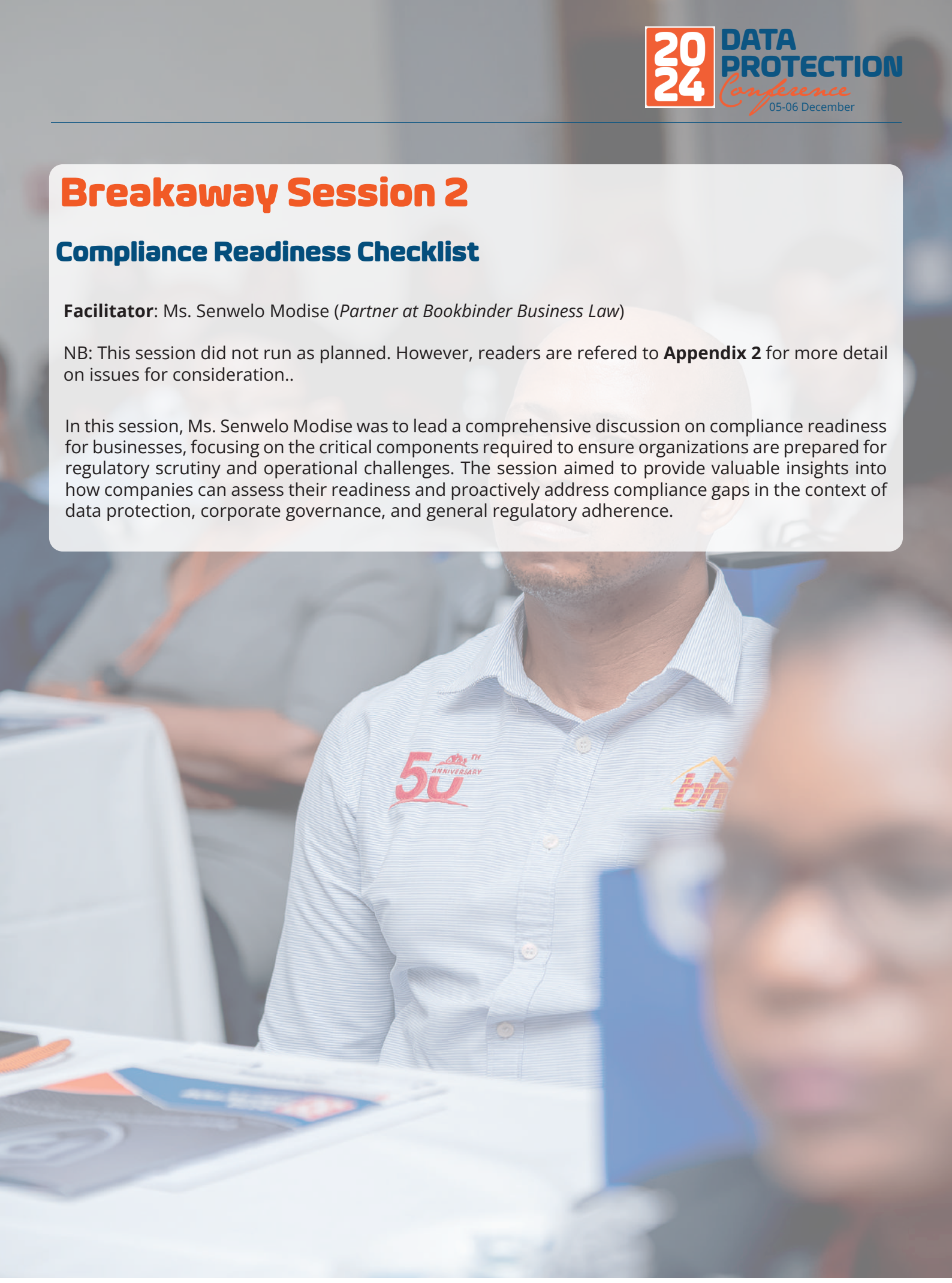
Breakaway Session 2

Compliance Readiness Checklist

Facilitator: Ms. Senwelo Modise (*Partner at Bookbinder Business Law*)

NB: This session did not run as planned. However, readers are refered to **Appendix 2** for more detail on issues for consideration..

In this session, Ms. Senwelo Modise was to lead a comprehensive discussion on compliance readiness for businesses, focusing on the critical components required to ensure organizations are prepared for regulatory scrutiny and operational challenges. The session aimed to provide valuable insights into how companies can assess their readiness and proactively address compliance gaps in the context of data protection, corporate governance, and general regulatory adherence.



SESSION 6

- **Panel Discussion 5**
  Data Protection in the Digital Age
- **Presentation 6**
  Bridging Borders: Botswana's Data Protection Bill in a Global Landscape:
- **Presentation 7**
  Contribution to the Successful Implementation of the Data Protection Act (DPA)-The Role of BoFiNet:
- **Closing Remarks**
- **Summary Highlights of the Conference**
- **IMPLEMENTATION CHALLENGES**
- **CHALLENGES EXPERIENCED AND ENVISAGED**
- **Appendix 1**
  Questions and Responses raised during the sessions
- **Appendix 2**
  Sample Compliance Readiness Checlist
- **Appendix 3**
  Conference Agenda

Panel Discussion 5:

Moderator:
Ms. Lebogang George (*Independent Consultant, Data Protection and Data Privacy Law Expert***)**

Panelist
Ms Ketshephaone Ngidi *(Botswana Data Protection Commission Office)*

Panelist
Professor Sizwe Snail *(South Africa Cyberlaw and AI Law Expert)*

Panelist
Mr. Paul Esselaar (*General Data Protection Regulation GDPR Expert***)**

Data Protection in the Digital Age

Introduction

Under the leadership of Ms. Lebogang George, the panel engaged in a robust discussion on the challenges, opportunities, and best practices for ensuring data protection in an increasingly digitized world. With contributions from legal, regulatory, and international perspectives, the discussion covered key issues ranging from compliance challenges to aligning local laws with global standards.

1. Botswana Data Protection Commission Office (Ms. Ngidi)

Ms. Ngidi opened the discussion by providing an overview of Botswana's data protection landscape, emphasizing the significance of the Data Protection Act (2018) in protecting individuals' privacy and ensuring responsible data use. She acknowledged the increasing complexity of safeguarding personal information in an era dominated by big data, artificial intelligence, and cross-border data flows.

Ms. Ngidi noted that while Botswana has made significant progress in setting up legal frameworks, enforcement remains a major challenge. Limited resources, inadequate awareness, and non-compliance by organizations hinder the full realization of the Act's objectives. She stressed the need for greater investment in capacity building, both within the Commission and among data controllers and processors.

She also addressed the issue of cross-border data transfers, stating that Botswana needs clearer guidelines on ensuring data sovereignty while enabling international data exchanges. Public education campaigns were another key recommendation, as many citizens remain unaware of their data protection rights.

Key Insight
Strengthening enforcement mechanisms and public awareness are essential for the effective implementation of Botswana's data protection laws.

2. Professor Sizwe Snail (South Africa Cyberlaw and AI Law Expert)

Professor Snail provided a comparative perspective, drawing on South Africa's experience with the Protection of Personal Information Act (POPIA) and other international data protection laws. He highlighted the challenges posed by emerging technologies like artificial intelligence, which often operate in legal grey areas where traditional privacy frameworks may not apply.

He debated the concept of "informed consent" in the digital age, arguing that users often consent to data use without fully understanding its implications. He suggested that data protection laws should move beyond consent-based models to incorporate principles of data minimization and purpose limitation more robustly.

Professor Snail also emphasized the importance of harmonizing regional data protection frameworks across Southern Africa. He suggested that Botswana could lead efforts toward creating a unified framework for the Southern African Development Community (SADC), like the European Union's GDPR, to facilitate seamless cross-border data flows while ensuring consistent protection standards.

Key Insight
Data protection frameworks must evolve to address emerging technologies and prioritize regional harmonization for cross-border effectiveness.

3. Mr. Paul Esselaar (GDPR Expert)

Mr. Esselaar brought an international perspective to the discussion, focusing on the General Data Protection Regulation (GDPR) as a global benchmark for data protection. He emphasized that while GDPR sets high standards, its principles can be adapted to local contexts like Botswana's. He praised Botswana's Data Protection Act for aligning with several GDPR principles, such as

transparency, accountability, and data subject rights. However, he pointed out areas where Botswana could improve, such as enforcement capabilities and penalties for non-compliance. He explained how GDPR's stringent fines have incentivized compliance in Europe and suggested Botswana could adopt a similar approach to deter violations.

Mr. Esselaar also highlighted the critical role of Data Protection Officers (DPOs), who serve as compliance champions within organizations. He recommended that Botswana mandate DPO appointments in certain sectors and invest in training programs to build local expertise in data protection.

Finally, he discussed the challenge of balancing innovation with regulation. He cautioned against overly rigid laws that might stifle technological advancements, advocating instead for a "regulate to innovate" approach that encourages compliance while fostering innovation.

Key Insight
Botswana can draw valuable lessons from GDPR by focusing on enforcement, penalties, and building expertise to enhance compliance.

4. Moderator's Reflections: Ms. Lebogang George

Ms. George synthesized the panellists' insights, emphasizing the common threads of enforcement, capacity building, and international alignment. She noted that while Botswana has a strong legal foundation, implementation challenges persist, and these need to be addressed urgently to keep pace with rapid technological changes.

She also opened the floor for debate on the potential risks of over regulation versus under-regulation, guiding the discussion toward finding a balance that supports both innovation and privacy. The panellists agreed that laws should be adaptive rather than static, with periodic reviews to incorporate emerging trends and technologies.

Ms. George concluded by challenging stakeholders to foster a culture of accountability and trust, emphasizing that data protection is not just a legal obligation but a cornerstone of ethical digital transformation.

The panel discussion underscored the importance of strong, adaptable, and well-enforced data protection laws in the digital age. With Botswana's Data Protection Act serving as a solid foundation, the panellists highlighted the need for enhanced enforcement, regional collaboration, and ongoing capacity building. By learning from international frameworks like GDPR and tailoring solutions to local needs, Botswana can position itself as a leader in data protection within the region. The discussion also emphasized the shared responsibility of regulators, businesses, and citizens in building a secure and privacy-conscious digital ecosystem.

Moderator and panelists of Panel Discussion 5: (Data Protection in the Digital Age)


ABB

Presentation 6

Bridging Borders: Botswana's Data Protection Bill in a Global Landscape:

By: Mr. Paul Esselaar (*South Africa Admitted Attorney, Data Protection / Privacy Law, Researcher in ICT Solutions***)**

Presenter: Mr. Paul Esselaar

Paul Esselaar's presentation, titled "Bridging Borders: Botswana's Data Protection Bill in a Global Landscape," provided a comprehensive examination of the challenges and opportunities presented by Botswana's Data Protection Bill. Drawing attention to specific sections of the Bill, Esselaar highlighted the practical implications for data controllers, data processors, and regulatory authorities, while addressing the capacity constraints Botswana faces in establishing a data protection framework that aligns with global standards such as the EU's General Data Protection Regulation (GDPR).

Esselaar began by outlining the implementation challenges articulated in Section 51 of the Bill. He noted that compliance would be particularly burdensome for data controllers, as each organization's implementation strategy would need to be uniquely tailored to its size, structure, and operations. This bespoke approach limits the possibility of replicating solutions across entities, further complicating compliance efforts.

A notable aspect of the presentation was Esselaar's discussion of the "Brussels Effect" and the emergence of what he referred to as the "Gaborone Effect." He explained that the GDPR has set a global benchmark, compelling organizations worldwide to adhere to its stringent standards. Similarly, Botswana's Data Protection Act has the potential to influence regional and international companies operating in or with the country. However, he stressed that achieving this regulatory influence would require Botswana to strike a balance between adopting stringent standards and ensuring that its laws are practical and workable for local entities.

Esselaar turned his focus to Section 4(2) of the Bill, which addresses jurisdiction and allows the Data Protection Commission to regulate entities outside Botswana that process data related to its citizens. He emphasized that this provision enhances Botswana's global reach and positions the country as a serious player in the international data protection arena. Additionally, Section 54, which mandates international businesses to designate a local representative in Botswana, provides a framework to facilitate accountability and enforceability for foreign entities.

On subcontracting, Esselaar highlighted Section 55, which restricts subcontractors from further subcontracting without general written

authorization. He pointed out that this clause underscores the need for robust oversight of third-party data processors to maintain data protection standards throughout the processing chain.

Addressing the Bill's provisions on audits, Esselaar noted that Section 58 requires data processors to notify the Commission of any contraventions of the Bill. While standard contractual clauses provided by the Commission may streamline compliance, the volume of audits and notifications is likely to challenge the Commission's capacity, particularly given the scale of data processing activities in Botswana.

Esselaar also discussed the Bill's data breach management requirements under Section 63, which stipulate that data controllers must report breaches within 72 hours unless deemed low risk. He raised concerns about the Commission's ability to handle potentially high volumes of notifications and the risk of delayed responses, which could escalate harm in the event of major breaches.

Privacy Impact Assessments (PIAs), as mandated by Section 68, were another focal point of the presentation. Esselaar emphasized that while prior consultation with the Commission is required for high-risk data processing activities, delays in responses from the Commission could hinder critical operations for businesses. This, he argued, underscores the importance of building a responsive and efficient regulatory body.

The role of Data Protection Officers (DPOs), outlined in Sections 69-73, was also discussed. Esselaar acknowledged the importance of these roles in ensuring compliance but raised concerns about Botswana's capacity to fill them, given the limited availability of trained professionals in the country. He emphasized the urgent need for capacity-building initiatives, including specialized training programs and partnerships with higher education institutions.

On international data transfers, Esselaar commended the Bill's provisions for adequacy decisions, binding corporate rules, and contractual clauses. However, he cautioned that the rigid nature of these mechanisms might pose challenges in maintaining flexibility to adapt to evolving international standards. He also highlighted Section 78, which permits exemptions under specific circumstances, warning that this could create regulatory loopholes if not carefully managed.

Esselaar concluded by emphasizing the significant effort required to build Botswana's data protection infrastructure. While the Bill provides a solid foundation, he acknowledged that Botswana lacks decades of experience held by regions like the EU. He recommended that the Commission take a proactive role in issuing guidance, promoting voluntary audits, and partnering with international bodies such as the European Data Protection Board (EDPB) and the UK's Information Commissioner's Office (ICO). These collaborations, he suggested, would provide Botswana with valuable insights and support in establishing a robust data protection regime.

Esselaar also asserted that the successful implementation of Botswana's Data Protection Bill would depend on the collective efforts of government entities, businesses, and international partners. Over time, he expressed optimism that Botswana would develop the capacity needed to meet the demands of the Bill while ensuring compliance from both local and international stakeholders. The Bill, he concluded, represents a significant step forward in modernizing Botswana's data protection framework and safeguarding the rights of data subjects.

Presentation 7

Contribution to the Successful Implementation of the Data Protection Act (DPA)-The Role of BoFiNet:

By: Shadrack Makhane (*Digital Delta Data Centre***)**

Mr Makhane led the discussion by asserting that the implementation of Botswana's Data Protection Act (DPA) of 2018 relies heavily on the contribution of key stakeholders, such as BoFiNet, a wholesale telecommunications and data infrastructure provider. Through its state-of-the-art infrastructure and services, BoFiNet plays a pivotal role in ensuring that Botswana achieves its data protection objectives, as mandated by the DPA.

Enhancing Data Security and Risk Management

He posited that BoFiNet's Digital Delta Data Centre (DDDC) is a cornerstone of its efforts to support the DPA. Operating under stringent security protocols, the DDDC ensures both physical and virtual protection of data. The Tier III certification by the Uptime Institute guarantees operational sustainability, minimizing the risk of data loss due to system failures or human errors. Additionally, enhanced physical security measures, such as restricted access, vehicle traps, and surveillance systems, prevent unauthorized entry into data storage facilities.

BoFiNet also prioritizes virtual security through its Points of Presence (PoPs) located in South Africa, Namibia, and the UK. These PoPs assist in filtering malicious traffic and reducing exposure to cyber threats, directly aligning with the DPA's mandate for safeguarding personal data.

Facilitating Compliance with Data Protection Regulations

Mr Makhane noted that BoFiNet provides infrastructure solutions that enable organizations to meet the compliance requirements of the DPA. To that end, Businesses can leverage BoFiNet's colocation services, hosting their data in a secure and vendor-neutral environment that aligns with international and local data protection standards. With Tier III Operational Sustainability standards and service-level agreements (SLAs) for power, cooling, and security, BoFiNet ensures operational transparency and reliability, enhancing organizations' ability to maintain compliance.

Supporting Digital Ecosystem Growth

He further submitted that BoFiNet's open-access model fosters digital transformation across Botswana. Its extensive national fiber network and interconnections with major international Internet Exchange Points (IXPs) reduce latency and increase data exchange efficiency. This infrastructure empowers businesses and government institutions to fulfill their DPA obligations while also driving economic growth and digital inclusivity.

By enabling secure, affordable, and high-speed connectivity, BoFiNet helps the government modernize Botswana's digital infrastructure and bridge the digital divide.

Promoting Business Continuity and Disaster Recovery

Mr Makhane apprised the participants that BoFiNet's colocation and interconnect services support organizations in ensuring business continuity and disaster recovery. Redundant power supplies and robust disaster recovery plans enhance the resilience of data storage and processing operations. These measures help organizations minimize downtime and risks associated with data breaches, enabling uninterrupted service delivery in compliance with the DPA.

Empowering Government Agencies

He noted that as a government-owned entity, BoFiNet plays a critical role in supporting public sector digital transformation. By housing sensitive

data locally at the Digital Delta Data Centre, the government ensures data sovereignty and compliance with national regulations. BoFiNet's secure infrastructure also facilitates collaborative efforts between government agencies and the private sector, further enhancing the implementation of the DPA.

Supporting National Goals

He said BoFiNet's initiatives align with the government's strategic objectives, including increasing digital inclusion, enhancing cybersecurity, and driving economic growth. By providing a secure and scalable ICT infrastructure, BoFiNet positions itself as an indispensable partner in Botswana's journey toward digital transformation and compliance with global data protection standards.

Implementation of Data Protection Laws in Ghana: Key Lessons: a Case Study

Mr Makhane proceeded to give an account of a case study of Ghana's implementation of its data protection laws and how Botswana can learn from Ghana's experience. He opined that Ghana's efforts to implement its data protection laws provide valuable insights into building a secure and compliant data ecosystem. By focusing on authorized access, compliance checks, robust enforcement, and proactive amendments to its Data Protection Act, Ghana has made significant progress in safeguarding personal data and fostering trust among stakeholders.

Strengthening Data Access Control

A cornerstone of Ghana's data protection framework is ensuring that only authorized personnel have access to sensitive information. To achieve this, organizations are required to implement advanced security protocols such as Privileged Access Management (PAM) and Multi-Factor Authentication (MFA). These measures are particularly effective in protecting Human Resources systems, reducing the risk of breaches and unauthorized manipulations.

Enhancing Compliance and Accountability

Ghana has established a comprehensive compliance framework to ensure adherence to data protection regulations. Regular audits, due diligence assessments, and investigations into complaints are conducted to identify and address any lapses in compliance. These activities not only promote accountability among organizations but also build public confidence in the regulatory framework.

Enforcing Data Protection Laws

Robust enforcement mechanisms are critical to the success of Ghana's data protection strategy. Regulatory authorities have the power to decline clearance for non-compliant data processing activities, suspend licenses, and impose sanctions on persistent violators. Workshops and educational campaigns are conducted to raise awareness among stakeholders, encouraging them to report suspicious activities such as phishing attempts.

In severe cases, authorities may even effect arrests to deter violations, demonstrating Ghana's commitment to upholding its data protection laws.

Proposed Amendments for Modern Challenges

Recognizing the need to adapt to emerging data challenges, Ghana has proposed amendments to its Data Protection Act. These include introducing new terminologies, such as privacy and cross-border processing, and mandating Data Protection Impact Assessments (DPIAs) for high-risk activities. These amendments aim to align Ghana's legal framework with international standards and ensure its relevance in a rapidly evolving digital landscape.

Collaboration and Public Awareness

The successful implementation of Ghana's data protection laws hinges on collaboration between

regulators, businesses, and the public. Increased public awareness and the expansion of regulatory operations to under served areas will further bolster compliance efforts, positioning Ghana as a leader in data governance within the region.

Conclusion

When winding his presentation, Mr Makhane concluded that Both Botswana and Ghana illustrate the importance of a comprehensive and collaborative approach to implementing data protection laws. While Botswana leverages robust infrastructure and partnerships through entities like BoFiNet, Ghana focuses on strengthening enforcement mechanisms and adapting its legal framework to modern challenges.

These efforts underscore the significance of fostering trust, ensuring compliance, and building capacity to safeguard personal data in an increasingly digital world. As Botswana and Ghana continue to refine their data protection strategies, they set a strong example for other African nations striving to establish secure and transparent data ecosystems.

"Delegates in attendance"

Closing Remarks

Professor Nkobi Pansiri (*BIBF Council Member*)

***Professor Nkobi Pansiri** (BIBF Council Member)*

As the conference concluded, Professor Nkobi Pansiri, a member of the Botswana Institute of Banking and Finance (BIBF) Council, expressed a sense of optimism alongside a clear understanding of the significant challenges faced by both Botswana and the broader region in achieving effective data protection and compliance. Reflecting on the discussions of the past days, Pansiri acknowledged the rich, insightful, and at times challenging nature of the sessions, which had provided valuable lessons that would guide the next steps in data protection.

Pansiri highlighted that the implementation of data protection laws is a complex and nuanced process, particularly in establishing new regulatory bodies such as the Botswana Data Protection Commission (BDPC). The creation of such a body requires meticulous planning, allocation of resources, and a firm commitment to ensuring that local regulations align with international standards. Emphasizing the importance of global best practices, particularly the General Data Protection Regulation (GDPR), Pansiri stressed that aligning Botswana's regulations with these standards was essential for the country to remain competitive in the digital economy and meet its international obligations.

One of the central themes that emerged during the conference was the pressing need for increased public awareness and education regarding data protection laws. Pansiri noted that while progress had been made in raising awareness, much work remained to be done. Both businesses and consumers must have a deep understanding of the significance of these laws and their respective roles in safeguarding personal data. Moving forward, it was crucial that efforts to educate and raise awareness continue, ensuring that all sectors, from small enterprises to large corporations, are adequately equipped to comply with the new regulations.

Pansiri also emphasized the role of technology as a critical enabler in implementing data protection laws. Despite challenges related to technological infrastructure and resource constraints, he underscored the importance of technology in improving compliance processes, enhancing security measures, and ensuring that data protection regulations are upheld effectively. Businesses must embrace technological solutions that can streamline compliance and protect sensitive information.

With the January 2025 deadline for full implementation of data protection regulations fast approaching, Pansiri stressed the urgency of the situation. He called for the BDPC to continue strengthening its capacity to monitor, audit, and enforce compliance. Additionally, he emphasized the need for clear guidelines and improved enforcement mechanisms to ensure that compliance is not merely aspirational but a

tangible reality. Pansiri also called for the support of businesses, particularly small and medium enterprises (SMEs), through resources, training, and guidance to help them meet the regulatory requirements.

Looking ahead, Pansiri emphasized the importance of a collaborative approach involving the government, regulatory bodies, businesses, consumers and educational Institutions. By working together, these stakeholders can create a culture of compliance that goes beyond legal obligations and fosters trust in Botswana's digital economy. While acknowledging the challenges that lie ahead, Pansiri expressed confidence that with concerted effort, innovation, and commitment, these challenges could be overcome.

In closing, Pansiri extended his heartfelt appreciation to all the panelists, speakers, and participants who contributed to the success of the conference. He expressed hope that the lessons learned would guide future efforts to build a secure and compliant data protection framework for Botswana. He called for continued engagement, collaboration, and innovation as the country works to meet the challenges and seize the opportunities ahead. He further expressed his gratitude for the initiative taken by the Botswana Institute Banking and Finance to bring together various stakeholders to dialogue on this issue of national importance and implored the BIBF to strive to be a key player in influencing policy in the banking and financial sector.

"Delegates in attendance"

Summary Highlights of the Conference

The conference provided a comprehensive platform for discussing key issues surrounding data protection, compliance, and technology law in Botswana. It brought together legal, cybersecurity, and compliance experts from various sectors, with a particular focus on the implementation of data protection laws considering advancements in technology and the introduction of new regulations.

Key highlights of the conference included:

i.Expert Panel Discussions: Panellists from a range of backgrounds, including legal, compliance, and cybersecurity sectors, discussed crucial topics such as AI, Big Data, Cybersecurity Law, and data protection compliance in Botswana's digital age.

Insights on Regulatory Challenges: Participants deliberated on the current challenges organizations face in complying with data protection laws, especially with the evolving technological landscape.

iii.Compliance Readiness: Key sessions focused on how organizations can assess their compliance readiness and adapt to emerging data protection frameworks such as the General Data Protection Regulation (GDPR).

iv.The Role of Technology: There were discussions about leveraging technology to enhance compliance processes, improve data protection measures, and facilitate the implementation of new laws.

"Delegates in attendance"

IMPLEMENTATION CHALLENGES

Several potential challenges to the implementation of data protection laws emerged from the discussions:

1.Complex Regulatory Landscape: The regulatory framework for data protection is still evolving, and businesses are struggling to keep up with changing requirements, especially those aligned with global standards like GDPR. This has created confusion among organizations on how to harmonize local regulations with international obligations.

2.Resource Constraints: Many businesses, especially SMEs, lack the technical and financial resources required to implement robust data protection systems. These include inadequate IT infrastructure, lack of qualified personnel, and insufficient budget allocation to establish compliance programs

3.Lack of Awareness and Education: A significant barrier to implementation is the low level of awareness about data protection laws among both businesses and consumers. Many organizations do not understand the nuances of compliance, leading to ineffective implementation strategies where there are efforts to do so.

4.Limited Technological Infrastructure: In Botswana, technological infrastructure in many sectors is still underdeveloped, posing a challenge to companies seeking to implement data protection and cybersecurity measures effectively.

"Delegates in attendance"

CURRENT STATUS QUO OF THE BDPC (BOTSWANA DATA PROTECTION COMMISSION)

i. The Botswana Data Protection Commission (BDPC) is still in the early stages of its operations. The BDPC is tasked with ensuring the implementation of the Data Protection Act. However, its ability to monitor and enforce compliance is limited by resources and technological capabilities. Some notable aspects of the current status quo include:

ii. Regulatory Framework in Place: While the legal framework for data protection was established, the BDPC is facing several challenges in terms of enforcement and ensuring widespread compliance across all sectors.

iii. Lack of Clarity on Specific Regulations: The BDPC has not yet issued comprehensive guidelines on many aspects of data protection, leaving businesses to navigate complex regulatory challenges on their own.

iv. Limited Awareness and Training: The BDPC is actively engaged in public awareness campaigns, but much work remains in educating the business community and the public about data protection rights and responsibilities.

v. Capacity Building: The BDPC has been working towards building its capacity, but it faces constraints in terms of qualified personnel, financial resources, and operational infrastructure.

THE 13TH JANUARY 2025 DEADLINE IMPLICATIONS AND MITIGATIONS

On the 13th January 2025, any entity that does not meet the minimum threshold for DPA compliance with be effectively and legally non-compliant. As the deadline for full implementation of data protection regulations approaches, there are several actions that need to be taken to ensure compliance:

Implications of the 13th January 2025 Deadline:

i.Non-compliance Risks: Organizations that fail to comply by the deadline may face legal penalties, reputational damage, and potential loss of business. This is particularly critical for companies involved in the digital economy and those processing sensitive customer data.

ii.Regulatory Pressure: The BDPC will likely increase its focus on compliance audits and enforcement, and businesses will need to be ready for scrutiny.

iii.Business Adaptation: For businesses to adapt successfully, they will need to overhaul their data protection practices and ensure they meet both local and international standards. Failure to do so could hinder their ability to operate in global markets.

Mitigations

1.Strengthening BDPC Enforcement Mechanisms: The BDPC needs to invest in enhancing its capacity to monitor, audit, and enforce compliance. This involves improving its technological infrastructure, building a team of skilled professionals, and establishing clear enforcement procedures.

2. Public Awareness Campaigns: A concerted effort must be made to raise awareness among businesses and the public about the importance of data protection, their rights, and obligations. The BDPC, in collaboration with industry bodies and training institutions like BIBF could lead national campaigns aimed at improving understanding of the Data Protection Act and its implications for businesses and individuals.

3.Guideline Issuance and Interpretation: The BDPC must urgently issue clear and practical guidelines on how businesses can meet compliance requirements, covering areas such as data collection, storage, processing, and cross-border data transfers. These guidelines

should also explain how businesses can address the specific challenges they face in implementing the regulations.

4.Capacity Building for Businesses: Organizations, especially SMEs, need assistance in preparing for the January 2025 deadline. The government and industry bodies could help by offering training, technical assistance, and resources to businesses struggling with implementation.

5.Leveraging Technology: Businesses should be encouraged to adopt technological solutions that can facilitate compliance with data protection laws, including automated compliance management systems, secure data storage solutions, and regular auditing tools.

"Delegates in attendance"

CHALLENGES EXPERIENCED AND ENVISAGED

During the conference, the following challenges were highlighted by various stakeholders, along with anticipated issues that could arise in the future:

1.Lack of Alignment Between International and Local Laws: The conflict between Botswana's data protection laws and international standards, such as the GDPR, remains a challenge. Companies involved in cross-border data transfer or multinational operations are struggling to align their local compliance efforts with global expectations.

2.Inadequate Data Protection Skills and Expertise: There is a shortage of qualified personnel with the expertise to implement and manage data protection strategies effectively. This is particularly concerning as the demand for skilled professionals in cybersecurity and data privacy continues to rise.

3.Technological Constraints: Many businesses do not have the technological capacity to secure data adequately, and there is insufficient investment in technological infrastructure that is capable of meeting regulatory demands.

4.Cultural Resistance to Change: Organizational culture can be a significant barrier to compliance. Resistance to change, especially in traditional sectors, makes it challenging for businesses to adopt new data protection policies and technologies.

5.Implementation Delays: As the deadline approaches, many businesses have yet to make substantial progress in their implementation plans, which could lead to delays and difficulties in meeting compliance by January 2025.

6.Legal and Regulatory Ambiguities: Some legal and regulatory frameworks remain vague or incomplete, creating confusion among businesses on how to navigate complex data protection issues.

INFERENCE FROM THE DELIBERATIONS

The conference highlighted the urgent need for collaborative action between the government, private sector, NGOs and regulatory bodies to ensure that Botswana is ready to meet international data protection standards by the January 2025 deadline. The shared challenges faced by stakeholders, such as limited resources, lack of awareness, and insufficient legal clarity, demonstrate the importance of proactive planning and capacity-building measures.

Moreover, the need for clearer regulatory guidelines, coupled with technology adoption and public awareness campaigns, will be critical to overcoming the hurdles to implementation. If businesses, public entities, the BDPC, and other stakeholders work in tandem, Botswana can move closer to achieving compliance and leveraging data protection as an enabler of trust and growth in the digital economy. However, without substantial efforts toward strengthening regulatory enforcement and supporting businesses, the risks of non-compliance could undermine the country's progress.


BRIGHT

Appendix 1

Questions and Responses raised during the sessions

Below is an extract of the many questions that were raised by the delegates during the sessions and the associated responses generated during question and answer sessions. It is anticipated that adopting the recommendations would go a long way in facilitating organisations to comply with the Data Protection Act.

i.How can organizations ensure ongoing compliance with the Data Protection Act in the face of rapidly evolving digital technologies?

• By regularly updating internal policies and training programs to address emerging technologies and

•Implementing continuous monitoring systems and conducting periodic audits to identify and mitigate potential data risks.

ii.What steps should be taken to ensure employees are adequately trained on data protection and privacy obligations?

Establish mandatory data protection training sessions, including phishing simulations and workshops. Reinforce these practices through periodic refresher courses to ensure continuous awareness.

iii.How can organizations protect sensitive supplier and customer data during the procurement process?

By implementing strict access control policies for supplier and customer data, requiring bidders and service providers to submit their data protection policies, and ensuring compliance with the Data Protection Act throughout the procurement lifecycle.

iv.What measures can be put in place to prevent unauthorized access to archived data?

Use encryption and secure storage systems for archived data. Implement role-based access controls and conduct regular audits to ensure that only authorized personnel have access to sensitive information.

v. How can organizations balance data protection requirements with the need for innovation and digital transformation?

• By incorporating data protection considerations into the design of new technologies and processes and

• Implementing privacy-by-design principles while ensuring that all digital transformation projects comply with the Data Protection Act to avoid security vulnerabilities.

vi. How can we ensure ongoing compliance with the Data Protection Act while keeping up with digital innovations?

•By regularly updating compliance frameworks to incorporate new technologies and data practices and

•Implementing a data protection impact assessment (DPIA) for new technologies to assess potential risks.

vii.What are the best practices for conducting data audits, and how often should they be performed?

Data audits should be conducted regularly, at least annually, to assess data handling practices, access controls, and security measures. Best practices include documenting audit findings and ensuring corrective actions are taken.

viii. How can we balance compliance with the Data Protection Act and the need for data-driven business strategies?

By implementing privacy by design principles, ensuring data protection is integrated into business processes and decisions, balancing innovation with compliance.

ix. What measures should we implement to ensure the secure storage and handling of sensitive data, both on-site and in the cloud?

Use encryption, access controls, and secure data storage protocols. Regularly audit cloud providers to ensure they meet compliance standards.

x. How can we mitigate risks related to third-party vendors and ensure their compliance with data protection policies?

By requiring third-party vendors to sign data protection agreements and conduct regular audits to ensure they meet compliance standards.

xi. What are the consequences of non-compliance with the Data Protection Act, and how can organizations avoid them?

Non-compliance can lead to significant fines, reputational damage, and legal consequences. Organizations can avoid this by continuously monitoring compliance and providing ongoing staff training.

xii. What steps should be taken to handle data breaches effectively and comply with breach notification requirements?

• Develop a data breach response plan, including notifying affected individuals and the regulatory authority within the required time frame.\

• Implement corrective measures to prevent future breaches.

xiii. How can organizations address the challenges of data protection in remote work environments?

By implementing secure virtual private networks (VPNs), enforcing strong authentication protocols, and providing training on securing personal devices.

xiv. How can organizations safeguard personal data during digital marketing campaigns and ensure compliance with the Data Protection Act?

By obtaining explicit consent from customers for data processing, anonymizing data where possible, and ensuring that marketing practices align with data protection principles.

xv. What specific policies should be created to protect employee data, and how can we ensure that all staff are trained on their rights?

Create policies for data access, retention, and security. Offer regular training sessions to ensure employees understand their rights and responsibilities regarding personal data.

xvi. How can the organization implement effective access controls to prevent unauthorized data access?

By using role-based access controls, multi-factor authentication, and regular reviews of access logs to ensure only authorized personnel access sensitive data.

xvii. What strategies can be employed to monitor and review the effectiveness of existing data protection measures?

Regular audits, continuous monitoring of security measures, and employee feedback can help assess the effectiveness of current data protection practices.

xviii. How do we ensure that sensitive data is properly anonymized or pseudonymized in accordance with data protection guidelines?

By implementing data masking and anonymization techniques, ensuring that sensitive data cannot be traced back to an individual without additional information.

xix. What role does transparency play in data protection, and how can it be implemented within an organization?

Transparency ensures trust. Communicate data protection practices clearly to employees and customers through privacy policies and regular updates.

xx. How can organizations ensure that customer data is securely processed, stored, and retained in compliance with data protection regulations?

By using secure systems for data processing and storage, implementing retention schedules, and conducting regular audits to ensure compliance with legal requirements.

xxi. What are the key legal risks associated with data protection that organizations must monitor?

Risks include breaches of confidentiality, unauthorized data access, non-compliance with data retention laws, and failure to notify data subjects about their rights.

xxii. How can organizations ensure that their data protection policies align with both local and international data protection laws?

By regularly reviewing and updating policies to reflect changes in both local and international regulations, and conducting cross-border compliance checks to align with GDPR, CCPA, etc.

xxiii. How can we establish clear data retention policies, and how do we ensure compliance with these policies?

By developing a retention schedule based on legal requirements and business needs, and ensuring employees follow these guidelines. Regular audits can ensure compliance.

xxiv.What role does employee awareness play in data protection, and how can organizations effectively educate their staff?

Employees must understand their role in protecting personal data. Offer ongoing training, phishing simulations, and refresher courses to keep staff informed.

xxv. How can organizations protect sensitive data during international data transfers?

By using data encryption, ensuring third-party compliance with data protection laws, and implementing Standard Contractual Clauses (SCCs) for cross-border transfers.

xxvi. What should organizations do to ensure that their data protection policies are up-to-date and compliant with new legislative changes?

Regularly monitor changes in data protection laws and update internal policies accordingly. Work with legal experts to ensure ongoing compliance.

xxvii. What tools or technologies can help organizations stay compliant with the Data Protection Act and mitigate potential risks?

Use data loss prevention (DLP) tools, encryption software, and compliance management platforms to track and manage data protection efforts.

xxviii. How can the Data Protection Officer (DPO) collaborate with other departments to maintain compliance and address data privacy concerns?

The DPO should be a key advisor, providing guidance on compliance, conducting regular training, and collaborating with IT, legal, and HR departments on data protection strategies.

xxix. What proactive steps can organizations

take to prevent cyberattacks and mitigate potential data breaches?

By regularly updating software and systems, conducting vulnerability assessments, implementing firewalls, and establishing an incident response plan.

xxx. How can organizations ensure that data protection is incorporated into the design and development of new products or services?

Integrating data protection into the product development lifecycle by adopting Privacy by Design principles, conducting DPIAs, and ensuring products meet data protection requirements from the start.

"Delegates in attendance"

Appendix 2

Sample Compliance Readiness Checlist

The compliance readiness checklist is a simple guideline on how organisation can approach and meet the DPA requirement to facilitate within their organisations.

This is not comprehensive, but presents the minimum it takes to comply with the respective DPA requirements. The organisation may choose a different approach provided that all the requirements are provided for.

Specific Requirement of the law	Provision in the DPA	Assessment of inherent risk			Governance and compliance framework* (Policies and procedures, including establishing governance structures, oversight and accountability mechanisms)		Alignment of ongoing activities to the requirements of the law* (Processes, controls and practices for effective implementation of the Act, policies and procedures)	
		Likelihood	Severity	Overall risk				
Lawfulness, fairness and transp	S.19, S.37	4	4	16	1. Data Protection Policy		1. Document the ROPA to establish the lawful grounds for processing personal data	FALSE
					2. Records of Processing Activities Procedure	FALSE	2. Inform data subjects about the processing of their personal data through Privacy Notices and any other viable means that ensure that the information is easily accessible, easy to understand and in clear and plain language.	FALSE
Purpose limitation	S.20	4	4	16	1. Data Protection Policy	FALSE	1. Document the ROPA to establish the purpose of processing personal data and sensitive personal data	FALSE
					2. Records of Processing Activities Procedure	FALSE		
Data minimisation	S.21	4	4	16	1. Data Protection Policy	FALSE	1. Document the ROPA to establish the personal data collected for each processing activity and whether it is strictly necessary to achieve the purpose(s) they were collected for.	FALSE
					2. Records of Processing Activities Procedure	FALSE	2. Review data collection medium and to eliminate the fields which result in the collection of personal data which are irrelevant and unneccesary to achieve the purpose of processing personal data.	FALSE
Information quality (Accuracy)	S.22	3	4	12	1. Data Protection Policy	FALSE	1. Review how personal data are collected and whether the manner of collection is likely to result in the collection inaccurate information. (e.g. collecting visitor information by asking questions instead inspecting a reliable identity document can likely result in the visitor giving incorrect/untrue information	FALSE
							2. Implement processes for updating personal data on regular intervals	FALSE
Retention limitation	S.23	3	4	12	1. Data Protection Policy	FALSE	1. Review the retention periods of personal data align with the requirements of the law, particularly that personal data is not stored for a period that is longer than necessary taking into account the purpose and significance of identifying the data subject for the particular processing.	FALSE
					2. Retention and Disposal Policy	FALSE		
Information security	S.24, S.62	4	4	16	1. Data Protection Policy	FALSE	1. Review the organisational and technical controls for effectiveness	FALSE
					2. Information Security Policy	FALSE		
							2. Establish Cybersecurity Maturity of the organisation	FALSE
Accountability	S.25	4	4	16	1. Governance structures	FALSE	1. Align the requirements of the law with the organisation's ongoing activities before the end of the transition period.	FALSE
					2. Data Protection Policy and associated policies indicated in this document)	FALSE	2. Conduct role-specific training	FALSE
					3. Data Protection Procedures (Procedures indicated in this document)	FALSE	3. Conduct enterprise wide training	FALSE
					4. Develop metrics to measure the performance of the compliance framework (Privacy Maturity Assessment Framework)	FALSE		
Legal basis for processing pers	S.26	4	4	16	1. Data Protection Policy	FALSE	1. Document the ROPA to establish the lawful grounds for processing personal data.	FALSE
Conditions for processing sensitive personal data	S.30 - S32	4	4	16	1. Data Protection Policy	FALSE	1. Document the ROPA to establish the appropriate condition for processing personal data sensitive personal data.	FALSE
Consent management	S26(1), S.27, S.28, S.30(2)(a)	4	3	12	1. Data Protection Policy	FALSE	1. Documented the ROPA to establish where consent will be used as a lawful grounds of processing personal data	FALSE
							2. Develop and implement processes for giving consent and withdrawing consent by the data subject.	FALSE

							3. Apply the consent process at every instance where consent is the lawful ground for processing personal data.	FALSE
Legitimate interest	S.26(f)	4	3	12	1. Data Protection Policy	FALSE	1. Document the ROPA to establish where legitimate interest is the lawful grounds of processing personal data	FALSE
					2. Legitimate Interest Assessment Procedure	FALSE	2. Conduct LIAs for every instance where legitimate interest is used as a legal basis. (e.g. CCTVs cameras, marketing)	FALSE
Access	S.42	3	4	12	1. Data Protection Policy	FALSE	1. Document the ROPA to establish the rights available to data subjects for each processing activity.	FALSE
Rectification	S.43	3	2	6				
Restriction	S.45,S46	3	2	6				
Objection	S.48	3	3	9				
Data Portability	S.47	2	3	6	2. Data Subject Rights Procedure	FALSE	2. Develop and document the process for the enforcement of these data subject rights	FALSE
Objection to decisions based solely on automated	S.49	3	3	9				
Erasure	S.44	3	3	9				
Direct collection	S.37, S.39, S.30	4	4	16	1. Data Protection Policy	FALSE	1. Place and/or present the relevant Privacy Notices at each data collection point.	FALSE
Indirect collection	S.37, S.40, S.41	4	4	16	1. Data Protection Policy	FALSE	1. Develop and document a process for informing data subjects whose personal data was not collected directly from them. (e.g. Next of Kin)	FALSE
Breach notification	S.63, S.64	3	4	12	1. Data Protection Policy	FALSE	1. Review incident management practices for effectiveness	FALSE
					2. Breach Notification Procedure	FALSE		
Confidentiality (unauthorised a	S.62	4	4	16	Refer to Information Security Principle	FALSE	Refer to Information Security Principle	FALSE
Integrity (unauthorised modification, alteration and	S.62	4	4	16	Refer to Information Security Principle	FALSE	Refer to Information Security Principle	FALSE
Availability (unauthorised restriction to personal data)	S.62	4	4	16	Refer to Information Security Principle	FALSE	Refer to Information Security Principle	FALSE
Appointment of DPO (including requirements for independence and reporting lines)	S.69 - S.72	3	3	9	1. Data Protection Policy	FALSE	1. Notify the Information and Data Protection Commission about DPO appointment	FALSE
					2. Appoint a DPO	FALSE	2. Develop training program/plan for the DPO	FALSE
Record of processing activities	S.60	4	5	20	1. Data Protection Policy	FALSE	1. Documented Record of Processing Activities	FALSE
					2. Records of Processing Activitities Procedure	FALSE		
Data Protection Impact Assessment (DPIA)	S.65 - S.67	4	4	16	1. Data Protection Policy	FALSE		
					2. Data Protection Impact Assessment Procedure	FALSE		
Prior Consultation	S.68	3	3	9	1. Data Protection Policy	FALSE		
					2. Data Protection Impact Assessment Procedure	FALSE		
Data Protection By Design and Default		3	4	12	1. Data Protection Policy	FALSE		
Legal basis for transfer of personal data outside Botswana	S.74 - 79	4	4	16	1. Data Protection Policy	FALSE	1. Document the ROPA to establish the lawful grounds for transfer of personal data outside Botswana.	FALSE
					2. Transfer Impact Assessment Procedure	FALSE	2. Conduct TIA for all transfers of personal data that are not based on adequacy	FALSE
In country storage of copy of personal data to be transferred	S.74	3	4	12	1. Data Protection Policy	FALSE	1. Copy personal data stored outside Botswana to infrastructure in Botswana	FALSE
Data processors	S.55 - S.58	3	3	9	1. Data Protection Policy	FALSE	1. Conclude Data Processing Agreements with all the vendors that process personal data on behalf of the organisation.	FALSE
					2. Data Processor Engagement Policy	FALSE	2. Conduct data processor due diligence to assess the sufficiency of their information security safeguards and compliance with the law.	FALSE
Joint controllers	S.53	3	3	9	1. Data Protection Policy	FALSE	1. Document the ROPA to identify the joint data controllers	FALSE
							2. Determine the arrangement with all the identified joint data controllers	FALSE
					Compliance status	0%	Compliance status	0%

Source: *Bookbinder Business Law*

NOTES:

1. Key Themes and Insights

The compliance readiness checklist underscores the importance of a systematic approach to compliance in today's regulatory environment where businesses must be proactive rather than reactive in managing their compliance obligations. The complexity of regulatory frameworks, especially in the context of data protection, necessitates that companies regularly review their compliance strategies to avoid fines, reputational damage, and legal repercussions.

2. Developing a Compliance Readiness Framework

The tool outlines the key steps businesses should take to assess their compliance readiness. She proposed a compliance readiness framework that includes the following components:

i.Regulatory Landscape Assessment: Understanding the current regulatory environment is the first step in ensuring compliance readiness. Organizations should assess applicable laws, industry regulations, and international standards to identify areas where they must comply, such as data protection, anti-money laundering, and cybersecurity laws.

ii.Internal Policies and Procedures Review: Businesses must ensure that their internal policies align with applicable regulations. Regular reviews of existing procedures, including data handling and privacy protocols, are essential for identifying gaps in compliance.

iii.Risk Assessment: Organizations should conduct a comprehensive risk assessment to identify areas of vulnerability in their operations, processes, and systems. Businesses need to not only identify regulatory risks but also evaluate financial, reputational, and operational risks related to non-compliance.

iv.Staff Training and Awareness: Ensuring that employees understand their roles in maintaining compliance is critical. Regular training programs should be implemented to educate staff about new laws, policies, and best practices related to data protection and other regulatory requirements.

Key Insight

With this robust compliance readiness framework, businesses can proactively identify risks, address compliance gaps, and align their practices with regulatory requirements.

3. Importance of Documentation and Record-Keeping

One of the key insights highlighted is the role of documentation and record-keeping in ensuring compliance. Businesses must maintain clear and accurate records of all compliance-related activities, including data protection assessments, employee training, and third-party contracts.

Proper documentation serves as proof that organizations are taking necessary steps to meet legal and regulatory requirements. In the event of an audit or regulatory investigation, having a well-organized compliance file could help avoid penalties or mitigate damage.

Key Insight

Maintaining comprehensive and accurate records of compliance activities is essential for businesses to demonstrate their adherence to regulatory requirements during audits or investigations.

4. Creating a Compliance Culture Within the Organization

There is need for organisations to embed a compliance culture within the organization. Compliance should not be viewed as an isolated function handled by the legal or compliance department, but rather as an integral part of the organizational culture. Management should lead by example, ensuring that compliance becomes a shared responsibility across all levels of the company.

To instil a strong compliance culture, businesses must:

i.Promote accountability at every level, ensuring that employees understand the importance of compliance in their daily tasks.

ii.Encourage open communication between departments to identify compliance issues and resolve them quickly.

iii.Develop a whistleblowing system that allows employees to report potential breaches without fear of retaliation.

Key Insight
Embedding compliance into the organizational culture ensures that it is seen as a shared responsibility, leading to more sustainable and effective compliance management.

5. Compliance Audits and Monitoring

It is important to conduct regular internal audits to assess compliance with existing laws and regulations. These audits should be structured, consistent, and result in clear action points to address non-compliance areas.

Continuous monitoring is key to ensuring ongoing compliance with the DPA. It's not enough to simply complete an audit and consider compliance as an ongoing task; businesses must have systems in place that monitor compliance continuously, especially in fast-changing regulatory environments. For instance, with data protection laws evolving globally, businesses need to ensure they are keeping pace with the latest regulations, such as the GDPR, and adjust their practices accordingly.

Key Insight
Regular audits and continuous monitoring ensure that compliance is not only achieved but sustained, helping businesses stay ahead of regulatory changes and reduce the risk of violations.

6. External Support and Expertise

Organisations should consider seeking external expertise to supplement in-house compliance efforts. For businesses lacking the resources or expertise to navigate complex regulations, partnering with external consultants or legal advisors specializing in data protection, cybersecurity, and regulatory compliance can be invaluable.

Organizations should regularly engage with legal experts, auditors, and compliance consultants to get updated on new legal frameworks and industry-specific compliance challenges. Moreover, that businesses should stay connected with regulatory bodies and industry associations to keep abreast of emerging compliance requirements.

Key Insight
External expertise and guidance can significantly enhance an organization's ability to stay compliant with complex regulatory frameworks and reduce the burden on internal teams.

7. Leveraging Technology for Compliance Management

Technology plays a significant role in managing compliance readiness. Digital tools, such as compliance management software, document management systems, and automated tracking tools, can be used to streamline compliance processes and reduce human error.

Businesses can also use AI and data analytics to track regulatory changes, assess risks, and generate reports automatically. Technology can significantly enhance the efficiency and effectiveness of compliance efforts by ensuring timely responses to regulatory updates and improving communication within the organization.

Key Insight
Leveraging technology can automate and streamline compliance tasks, reduce the risk of errors, and improve efficiency in compliance management.

Compliance readiness is a continuous, evolving process rather than a one-time effort.

Businesses must therefore remain proactive in monitoring their compliance status, staying informed about regulatory changes, and continuously adapting their policies and processes to meet new challenges.

"Delegates in attendance"

Key Takeaways

i. A compliance readiness framework is essential for identifying gaps and proactively addressing regulatory risks.

ii. Documentation and record-keeping are crucial for demonstrating compliance during audits and inspections.

iii. Embedding a compliance culture across the organization helps ensure that compliance is seen as a shared responsibility.

iv. Regular audits, continuous monitoring, and external expertise are key to maintaining compliance over time.

v. Technology plays a crucial role in automating compliance tasks and improving efficiency.

Businesses should therefore consider compliance readiness not as a regulatory burden, but as a strategic priority that enhances operational resilience, protects the organization's reputation, and ultimately supports sustainable business growth.

"Delegates in attendance"

Appendix 3

Conference Agenda

Directors of Ceremony

Leene Nage: Business Development, Marketing and Partnerships Manager at BIBF

Pearl Leburu: Relationship Manager SME Banking at Standard Chartered Bank

DAY 1 , DECEMBER 5 2024

TIME	SESSION	SPEAKER/ FACILITATOR
07:00 - 08:00	Registration	
08:00 - 08:15	Arrival of guests	
	Session 1: Opening Session	
08:15 - 08:20	Opening prayer	**Mr Segomotso Mosokotso** (BIBF Sales Officer)
08:20 - 08:30	Welcome remarks	**Mr Molaodi Menyatso** (BIBF Managing Director (Ag))
08:30 - 08:45	Opening Remarks	**His Honor Mr Ndaba Gaolathe** (Republic of Botswana Vice President & Minister of Finance)
08:45 - 09:15	Data Protection In Botswana	**Botswana Data Protection Commission**
09:15 - 09:45	Keynote address	**Professor Sizwe Snail** (Keynote speaker Cyberlaw and AI Law expert, Admitted Attorney in South Africa and former member of Information Regulator, Contributor to South Africa POPIA Law)
	Session 2: Presentations 1	
09:45 -10:15	Overview of the DPA, the new amendments & implications of non-compliance	**Ms Lebogang George** (Independent Consultant, Data Protection and Data Privacy Law expert)
10:15 - 10:30	QUESTIONS & ANSWERS	Delegates
10:30 - 11:00	Coffee break	
11:00- 11:30	Evolution of Data Protection Laws (Global / International Context)	**Mr Kgotso Botlhole** (Managing Partner Botlhole Law Group) Conference Diamond Sponsor
	Presentations 2	
11:30 - 12:00	Data Protection Through the Lens of Judicial Decisions	**Ms Senwelo Modise** (Partner at Bookbinder Business Law)
	Session 3: Panel discussion	
12:00 - 13:00	Role of data protection in media & communication	**Moderator ;Mr Fungai Mazarura** (Business and Public Relations Consultant at Akheel Jinabhai & Associates in Association with Mckee Commercial Law) **Panelist; Spencer Mogapi** (Former Editor at Sunday Standard Communications Expert) **Mr Igamu Bonyogo** (Corporate Legal Advisor, Kingsway Consultancy) **Simon Bathusi** (Partner at Armstrongs) **Shathani Molefe** (Chief Compliance Officer, Standard Chartered Bank)
13:00 - 14:30	Lunch break	

Session 3: Panel discussion		
14:30- 15:30	The Future of Data Protection in the Age of AI and Big Data	**Moderator ;Professor Sizwe Snail** (South Africa Cyberlaw and AI Law expert) **Panelist; Mr Tumelo Bethuelson** (Manager, Business Intelligence at FNBB) **Mr Thabiso Oabile** (Chief Technology Officer, Botswana Insurance Company) **Dr Bokamoso Basutli** (Snr. Lecturer, Department of Electrical, Computer, and Telecommunications Engineering, BIUST and BOCRA Board Member)
15:30- 16:15	Data Protection Compliance in the Digital Banking Age	**Moderator ;Ms Sedilame Modiga** (Manager, Business Compliance Advisory, Stanbic) **Panelist; Ms Lorato Kgosidiile** (Associate Attorney, Botlhole Law Group) **Ms Kutlwano Tatolo** (Bofinet Legal Counsel and Board Secretary) **Mr Petros Molefe** (Chief Information Officer, Standard Chartered Bank)
16:15-16:45	Questions & Answers and wrap of DAY 1	

DAY 2 ,DECEMBER 6 2024		
TIME	**SESSION**	**SPEAKER/ FACILITATOR**
07:00 - 08:15	Registration	
08:15 - 08:30	Arrival of guests	
Session 4: Opening Session		
08:30 - 08:35	Opening prayer	**Mr Segomotso Mosokotso** (BIBF Sales Officer)
08:35 - 08:45	Recap of DAY 1	**Ms Lebogang George** (Independent Consultant, Data Protection and Data Privacy Law expert)
Session 5: Presentations		
08:45 - 09:30	Implementation of DP Laws in Ghana, Implementation & Enforcement. as the first DP Commissioner, strides made	**Dr Patricia Poku** Data Protection Office, Ghana
09:30 - 10:15	GDPR as International best practise	**Mr Paul Esselaar** (South Africa Admitted Attorney, Data Protection / Privacy Law, Researcher in ICT Solutions)
10:15-10:30	Questions & Answers and wrap of DAY 1	

TIME	SESSION	SPEAKER/ FACILITATOR
10:30 - 11:00	Coffee break	
	Session 6: Panel discussion	
11:00 - 12:00	Cybersecurity law, technology law	**Moderator ;Professor Sizwe SnaiL** (South Africa Cyberlaw and AI Law expert) **Panelist; Dr June Jeremiah** (Director & Cybersecurity Engineer, MCS Security Solutions Pty Ltd) **Mr Martin Kamethu** (Head of Operations, Serianu Limited, Botswana Office) **Ms Segametsi Mafa** (Managing Director Service Xcellence, IT & Corporate Governance, Board Memeber BSE) **Mr Pako Phatsimo** (Technology Risk and Governance Manager, FNBB)
	Move to breakaway rooms	
	Breakaway sessions	
12:00 - 13:00	Leveraging off technology to ensure compliance and implementation of Data Protection	**Mr Fred Webb** **(Compliance Lead, Debswana)**
	Compliance readiness checklist	**Ms Senwelo Modise** **(Partner at Bookbinder Business Law)**
13:00 -14:30	Lunch break	
	Session 7: Panel discussion	
14:30 - 15:30	Data Protection in Africa: Lessons learned from other African countries, lessons learned from the EU, Strengthening data protection In Africa: key issues for implementation, how can lawmakers improve data protection and address the current gaps in some of the DP legislation	**Moderator ;Ms Lebogang George** (Independent Consultant, Data Protection and Data Privacy Law expert) **Panelist;Botswana Data Protection Commission** **Dr Patricia Poku** (Data Protection Office, Ghana) **Mr Paul Esselaar** (GDPR) **Professor Sizwe Snail** (South Africa Cyberlaw and AI Law expert)
15:30 - 16:00	Questions & Answers and wrap of DAY 2	
16:00 - 16:10	Closing remarks / Vote of thanks	**Professor Nkobi Pansiri** **(BIBF Council Member)**
17:00 - 20:00	Cocktail and networking dinner	

Botswana Institute of Banking & Finance

Transforming future capability

Data Protection Conference

Law, Compliance, Risk Management

For more information and to register,

please contact Botswana Institute of Banking and Finance

(BIBF) at

Phone Number: 395 2493 Email Address: enquiries@bibf.ac.bw

Website URL: www.bibf.ac.bw