Data Protection and Privacy - Key Data Privacy and Compliance Trends of 2022

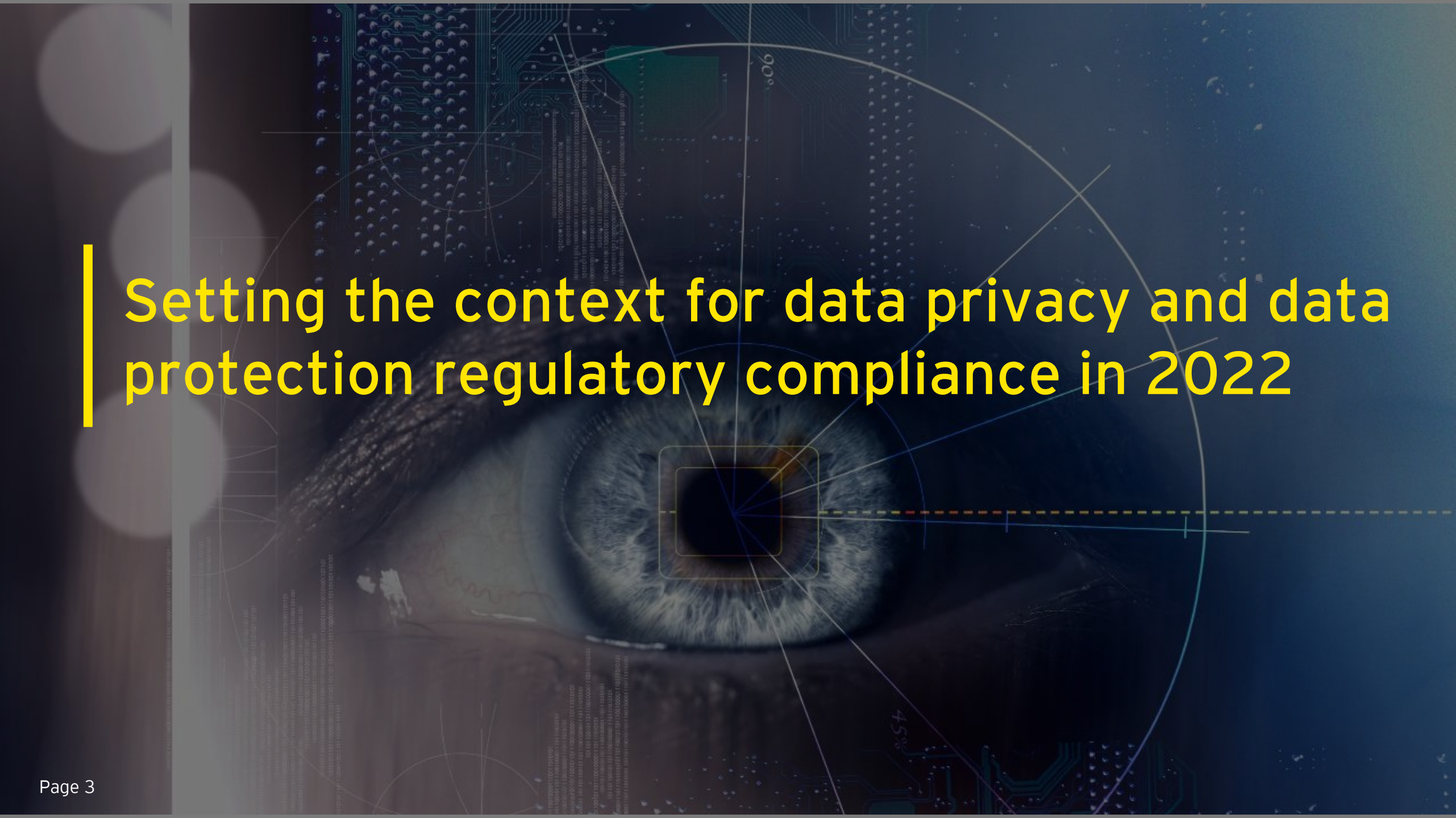
Chief Compliance Officers Retreat 2022

Association of Chief Compliance Officers of Banks in Nigeria

February 2022

What I plan to speak about …

1. Setting the context for data privacy & protection regulatory compliance in 2022
2. What trends do we see for 2022?
3. Implementation approach and methodology towards compliance
4. Key success factors for successful data privacy & data protection implementation



Setting the context for data privacy and data protection regulatory compliance in 2022

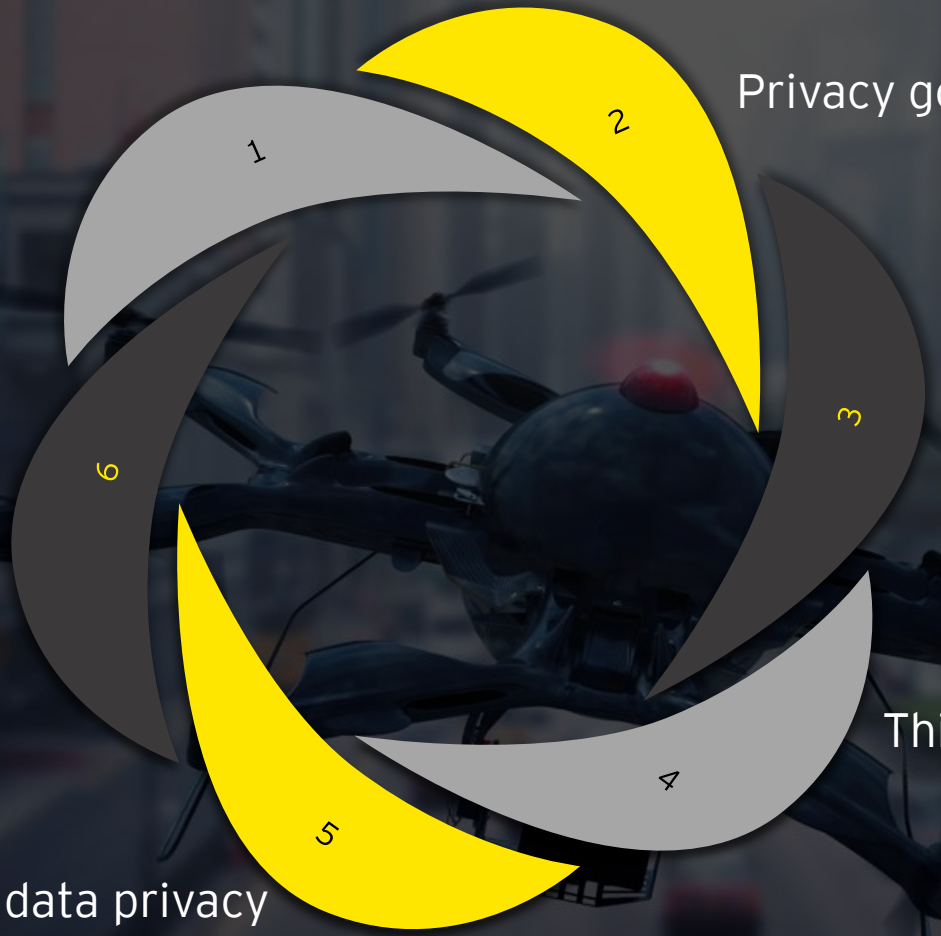
Compliance with data privacy and data protection regulations is not primarily about keeping on the right side of regulators — it's an opportunity to create business value while managing risk now and into the future

Benefits of compliance with data privacy & data protection regulations

- Enhanced cyber security
- Improved data management
- Optimised internal processes
- Boost in customers' and other stakeholders' confidence
- Provides competitive advantage
- Right side of the law

What trends do we see for 2022?

What trends do we see for 2022?



Know your new sheriff …
Nigeria Data Protection Bureau

Privacy goes global

More use of Governance,
Risk & Compliance software

Third party risk management

More transparency of data privacy

Privacy Tech

Know your new sheriff … Nigeria Data Protection Bureau

- Carved out of NITDA in February 2022
- Pioneer National Commissioner/Chief Executive Officer is ex-NITDA … since 2002
- What should we expect?
  - Filing deadline of data privacy audit reports extended to 30 June 2022
  - DPCOs need to become familiar with the operations of the Bureau
  - What else?

Privacy goes global

- Regulators are demanding more from businesses, with strict guidelines as the world is trying to introduce or increase its data management, policies, and privacy schemes.
- Following new regulations is of utmost importance for businesses, with those who fail facing sanctions and litigation.
- After a few “quiet” years with a small number of fines, the cases filed with the various data protection authorities have worked their way through the system and the increase in fines reported in 2021 will likely continue.
- Nigeria is considering a Data Protection Act. Canada and Australia are updating their privacy laws, India is considering a new privacy law, China will be enforcing the law it passed in 2021, and Saudi Arabia (among other countries) passed a privacy law in 2021.

Privacy goes global (cont'd)

- Updates from EU GDPR are worth mentioning - during 2021 summer, European Commission released new Standard Contractual Clauses (SCCs), which focus on transfer of personal data from EU to third countries. New laws and amendments will become operational within 2022, meaning the time left to meet the requirements is swiftly running out.

- Businesses should prepare themselves and set up a plan to assess applicability of data privacy laws/ regulations, together with a schedule for company adjustments in order to comply.

- This will require businesses to create (if they haven't already) comprehensive privacy programmes that allow them to understand what personal data they collect, where it sits, how they use it, who they share it with, and the value of that data. This is not a one-time exercise; it will require ongoing maintenance.

More use of Governance, Risk & Compliance software

- GRC software has become a necessity for businesses - aids organisations to manage the necessary documentation, while also preventing vulnerabilities that could impact the organisation.
- The need to be ready should be top priority for any organisation as failing in this area could affect systems, resources and stakeholders.
- New GRC management smart Artificial Intelligence programmes will help to reduce the risk time due to the speed of the automated response.

Third party risk management

- Focuses on identifying and reducing the amount of risks involved in using third party services.
- With ransomware threat on the rise, organisations should perform effective due diligence when it comes to opening their businesses up to include third-party vendors.
- In many cases, third party risks are identified after completion of initial onboarding – failures to identify threats in advance resulted in some notable breaches during 2021.

More transparency of data privacy

- Due to media coverage on data privacy failures, people are now more aware than before on privacy laws.
- More consumers will become more interested in what personal data organisations hold about them and the purposes of the processing.
- There is much less trust when it comes to social media and tech companies collecting data. There needs to be much more concentration by businesses now to be transparent and earn that trust back.
- Whither Cookies and privacy preferences:
  - After years of consumers happily surfing the web and using apps with reckless abandon, data privacy became a “thing” in 2021.
  - People got wake-up call when their favorite apps and websites started asking them to agree to cookies or to make their privacy preferences known — a reminder that organisations track their online behaviors.
  - But it was not only consumers who had to think about data privacy. Many companies had to reconsider (or consider for the first time) their data privacy practices. Some even had to pay up (fines) due to their practices.

Privacy Tech

- As regulators, consumers, etc., continue to put pressure on business models that rely on the sharing of personal data, businesses will turn to technology to help them achieve their business goals
- 2021 witnessed the rise of privacy-enhancing technologies … they will take centre stage in 2022
- Techniques like differential privacy* and homomorphic encryption**, along with solutions that involve synthetic data,*** will gain in popularity as sharing personal data continues to be hindered by privacy-related restrictions
  - Companies should expect to see more of these solutions being marketed to them and will need to understand the technology and its implications as they decide which to add to their inventory.

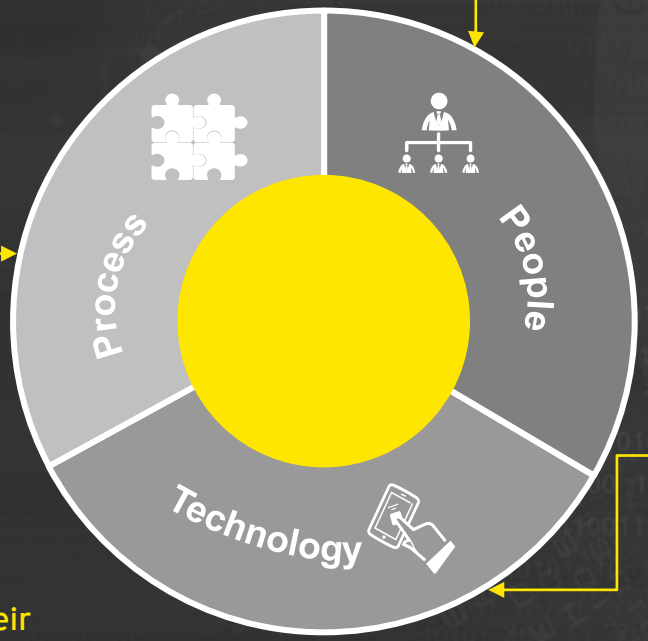
* Differential privacy is a system for publicly sharing information about a dataset by describing the patterns of groups within the dataset while withholding information about individuals in the dataset.

** Homomorphic Encryption refers to a special type of encryption technique that allows for computations to be done on encrypted data, without requiring access to a secret (decryption) key. The results of the computations are encrypted, and can be revealed only by the owner of the secret key.

*** Synthetic data are generated to meet specific needs or certain conditions that may not be found in the original, real data. This can be useful when designing any type of system because the synthetic data are used as a simulation or as a theoretical value, situation, etc.

Implementation approach and methodology towards compliance

NDPR is transformational, touching on all aspects of an organisation



People

- NDPR will require organizations to **adequately train personnel** responsible for handling personal data to ensure NDPR compliance.
- Organizations will need to **identify the relevant stakeholders** across business units who can contribute to compliance remediation planning and execution.

Process

- Organizations will need to determine which **business processes are impacted by NDPR** requirements.
- NDPR will require organizations to **redesign their processes** to incorporate steps that address key privacy requirements.
- Organizations must **implement process monitoring controls** to affirm that the processes consistently satisfy NDPR requirements and are updated as necessary.

Technology

- Organizations must understand their IT environment, data assets and data processing applications to identify the impacts that NDPR requirements present and to **develop a remediation plan to update the IT environment** to support NDPR compliance.
- Organizations should look into various **tools available for automating** NDPR compliance operations to an enterprise scale.

Implementation methodology

EY utilises EY's data privacy framework and NDPR implementation framework to assess personal data management practices

Programme

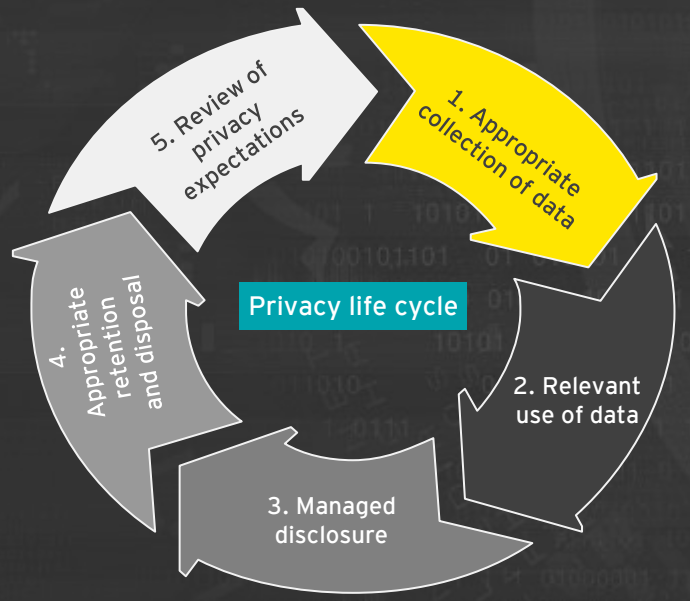
Privacy strategy/charter	Regulatory reporting
Privacy policy	Executive reporting
Training and awareness	Managing public perception

Supporting Governance Roles

- IT Governance
- Legal and compliance
- Communications and crisis management

Operations

- Privacy by design
- Risk management
- Incident management
- Vendor due diligence
- Consumer request/complaints
- Data classification
- Personal data Inventory Management
- Cross border data management



Managed Lines of Defense

DPO

Risk and compliance

Audit

Monitoring

Regulatory expectations	Privacy audit
Internal expectations	Data flow management

- Data owners
- Data processors
- Data collectors

Key success factors for successful data privacy & protection implementation

Building organisational capability

1

Clear Vision

Setting a clear vision of what data privacy and data protection compliance look like is key. This allows the change programme to focus resource effectively and target a specific desired state. If a clear vision isn't set, the programme will be obligated to set its own vision, costing time and energy.

2

Sponsorship

Visible executive sponsorship demonstrates organisation buy-in and accountability. A clear principle of on-going data privacy and data protection compliance activities. Having a clear escalation structure helps navigate the organisational challenges that NDPR and similar regulations can create

3

Business/IT Engagement

Interpretation of data privacy and data protection regulations is sometimes considered an IT issue to resolve. Whilst IT change is required, the regulations touch business process and people change, requiring a holistic approach to compliance

4

Programme Governance

As compliance hots up, organisations are adopting new programme methods such as Agile. These should be implemented carefully to ensure efficiency and traceability

5

Budget / Prioritisation

Budgeting and prioritising according to a risk based approach is key. Data privacy and data protection regulatory compliance is a broad topic; demonstrable compliance and a clear approach is key

19

Bringing it all together …

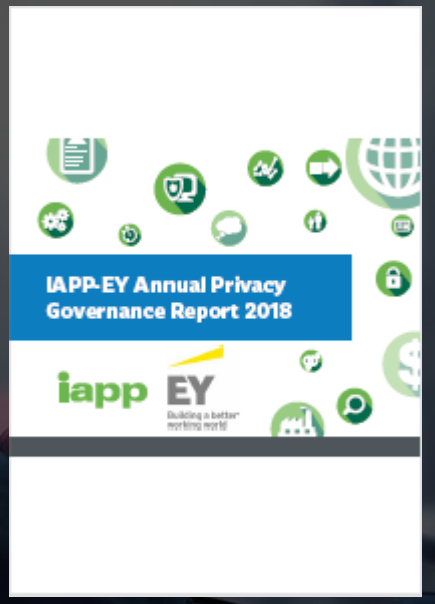
NDPR and allied regulations impact nearly every facet of an organization. As a result, they present an opportunity for most organisations to fundamentally transform and improve their internal processes and drive more effective utilisation of data while enabling compliance.

A transformative year is in the horizon … will Nigeria join the league?

Additional resources for you

When is privacy not something to keep quiet about?

Privacy trends 2016: Can privacy really be protected anymore?

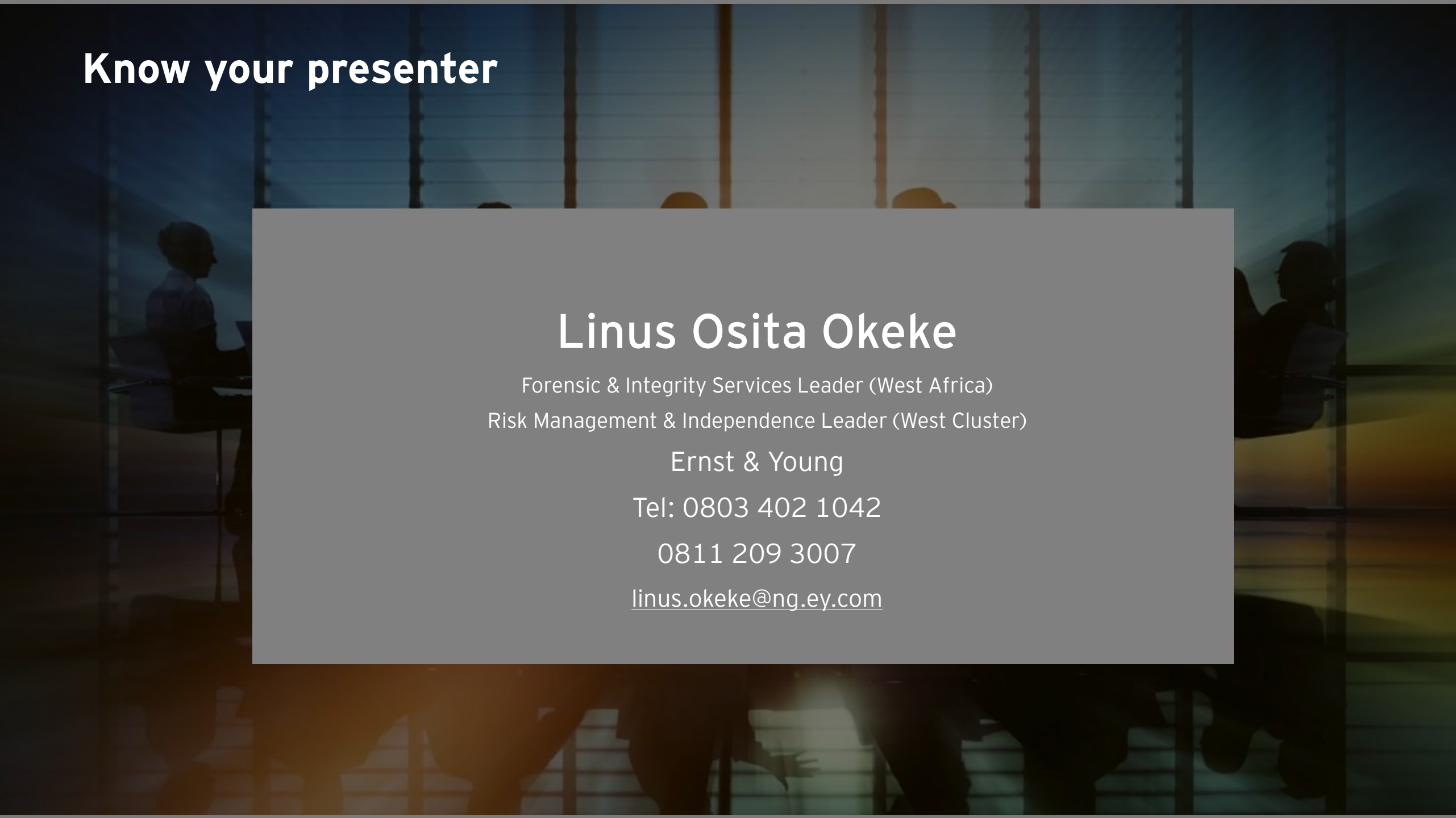


IAPP-EY Annual Privacy Governance Report 2018

EU General Data Protection Regulation: are you ready?

Please visit ey.com/cyber for information about data protection and privacy and more.

Know your presenter



Linus Osita Okeke

Forensic & Integrity Services Leader (West Africa)

Risk Management & Independence Leader (West Cluster)

Ernst & Young

Tel: 0803 402 1042

0811 209 3007

linus.okeke@ng.ey.com