ORARO & COMPANY
ADVOCATES

An Affiliate Member of AB & DAVID AFRICA

Data Protection

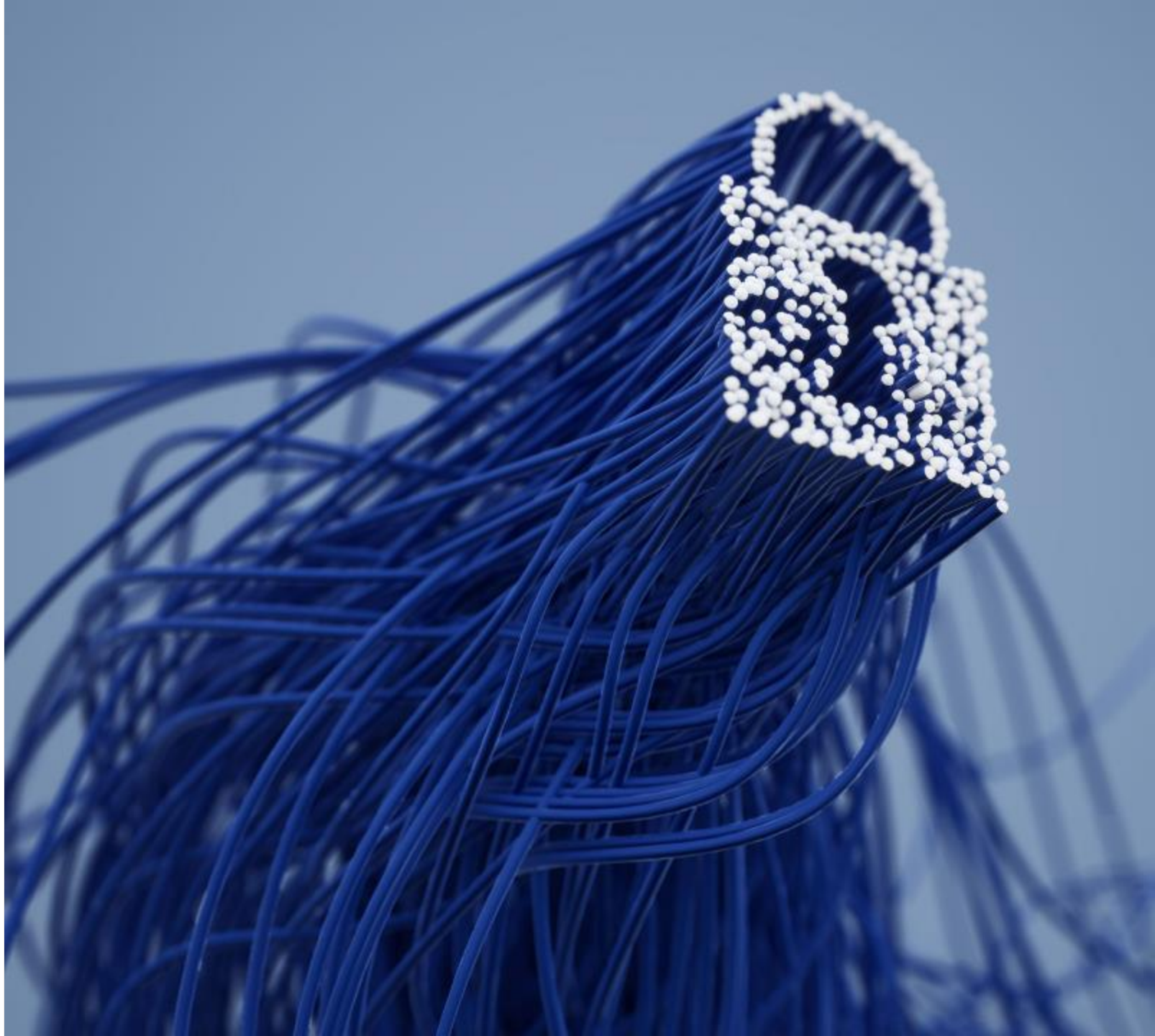
22nd July 2021

Presented by: John Mbaluto, FCIArb

Jacob Ochieng,

Daniel Okoth &

Milly Mbedi



About Us

- Oraro & Company Advocates is a **top-tier**, full-service law firm in Nairobi, Kenya established in 1977.

- We provide specialist legal services both locally and regionally in **Arbitration, Asset Tracing & Recoveries, Banking & Finance, Capital Markets, Conveyancing & Real Estate, Corporate & Commercial, Dispute Resolution, Employment & Labour, Fintech, Infrastructure, Projects & PPP, Restructuring & Insolvency** and **Tax**.

- We have also been consistently ranked and recognised by Chambers Global, IFLR 1000 and Legal 500 as a top-tier firm.

The Legal 500 EMEA TOP TIER 2021

TOP RANKED Chambers Global 2021 Oraro & Company Advocates

IFLR 1000 RECOMMENDED FIRM 30th EDITION

About the Speakers

John Mbaluto, FCIArb

DEPUTY MANAGING PARTNER

A Partner at the Firm's dispute resolution practice group, John specialises alternative dispute resolution and litigation. He has built a respected legal career spanning over 12 years, having represented and advised local and international clients particularly in employment and labour law, pension law, construction law, banking and commercial disputes and constitutional law.

John very recently attained qualification as a Fellow of the Chartered Institute of Arbitrators (FCIArb), a globally recognised standing in arbitration circles.

E: john@oraro.co.ke

Jacob Ochieng

PARTNER

Jacob is a Partner at the Firm's corporate & commercial practice group. With over 10 years' experience, he has advised local and international corporates on infrastructure projects, commercial contracts, corporate restructuring, mergers & acquisition and privatisations.

Chambers Global ranked Jacob its 2020 Guide under Corporate/M&A and commented that he "*is commercially astute and always looks out for his clients in any transaction*."

E: jacob@oraro.co.ke

About the Speakers – Contd.

Daniel Okoth

PARTNER

Daniel is a Partner in the dispute resolution practice group. With over 7 years' experience, Daniel has advised local and international clients from various sectors including financial services, education and real estate in arbitration, banking and commercial litigation, constitutional and administrative law,, employment & labour law disputes and land disputes.

E: daniel@oraro.co.ke

Milly Mbedi

SENIOR ASSOCIATE

Milly is a Senior Associate in the firm's corporate and commercial practice group and specializes in corporate & commercial law, competition law, employment & labour law and intellectual property law. With over 7 years' experience, she has advised both local and international clients from various sectors on corporate restructurings, mergers & acquisitions, commercial contracts, drafting employment contracts, reviewing of employment policies & procedures and trademark and copyrights.

E: milly@oraro.co.ke

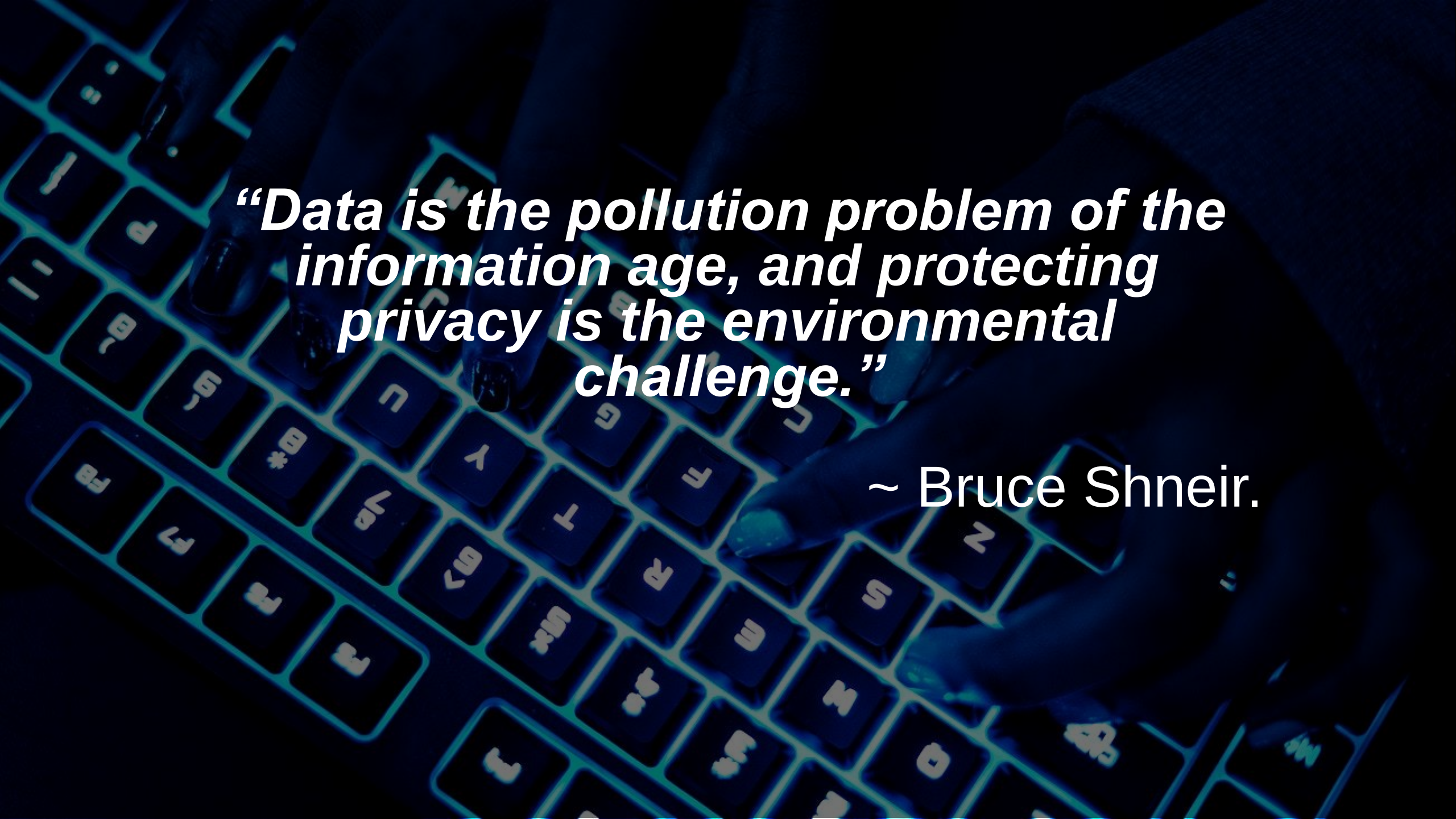
In this presentation

a) Background to the Data Protection Act, 2019 (the "**Act**" or "**DPA**")

b) An Overview of the Salient Provisions of the Act

c) Jurisprudence & Conclusions

d) Q & A


“Data is the pollution problem of the information age, and protecting privacy is the environmental challenge.”
~ Bruce Shneir.

Background to Data Protection Act, 2019

- The Constitution of Kenya, 2010 has been heralded for its robust Bill of Rights which, among other rights, introduced the right to privacy.
- **Art. 31**, provides as follows: -
  - Every person has the right to privacy, which includes the right not to have-
    a) …. ;
    b) …;
    c) information relating to their family or private affairs unnecessarily required or revealed; or
    d) the privacy of their communications infringed.

- Courts in Kenya have been enforcing Art. 31 by upholding the principles of data protection e.g. the need to balance the right to privacy with the greater public interest, consent as a defence, etc

Background to Data Protection Act, 2019 – Contd.

- Globally, there had been an ongoing conversation around data protection arising from the public concern about personal privacy in the face of rapidly developing computer technology.

- More widely in Europe, the EU made General Data Protection Regulations (**EUGDPR**) on 14th April 2016 which came into force in May 2018.

- This was followed by the UK remodelling its existing Data Protection legislation with the passage of the **UKDPA** (2018).

- The fragility of personal data and its susceptibility to abuse was exposed with **the Cambridge Analytica Scandal** in early 2018 where personal data of Facebook Users is alleged to have been harvested without consent for political advertising.

Background to Data Protection Act, 2019 – Contd.

Some of the salient features of the EUGDPR are;

- Expanded Territorial scope under Articles 3(2) and 3 (3): it covers non-EU jurisdictions in which the personal data of EU subjects is transferred.
- Significantly onerous **penalties** i.e. 4% of annual global turnover or up to 20 million Euros (whichever is higher).
- Data breaches must be reported to the relevant regulator without undue delay: within 72 hours of becoming aware of a breach.
- Organizations relying on Consent to process data have the burden of demonstrating that Consent was freely given.
- Obligation to carry out Data Protection Impact Assessments.
- Contains rights around data portability, the right to be forgotten and to prevent profiling; the right to object to processing, to rectification and erasure.
- Privacy by Design or Default. Prohibits pre-set defaults for disclosure to all.
- Data processing must be carried out for the original purpose for which it was collected.

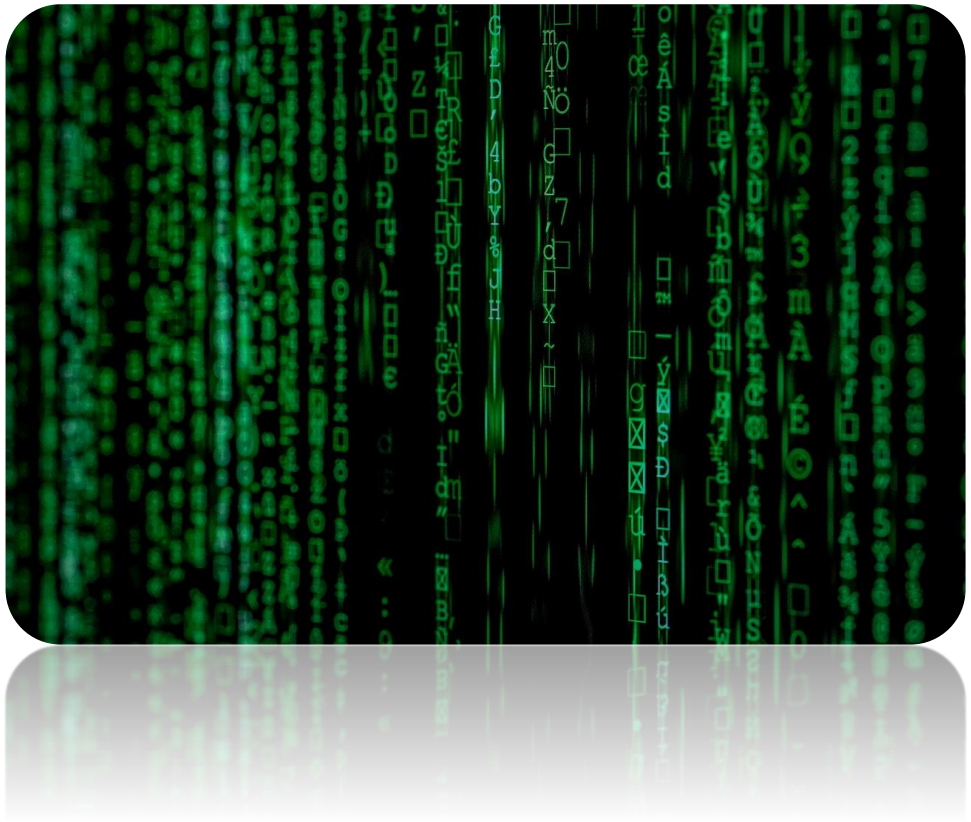
Background to Data Protection Act, 2019 – Contd.

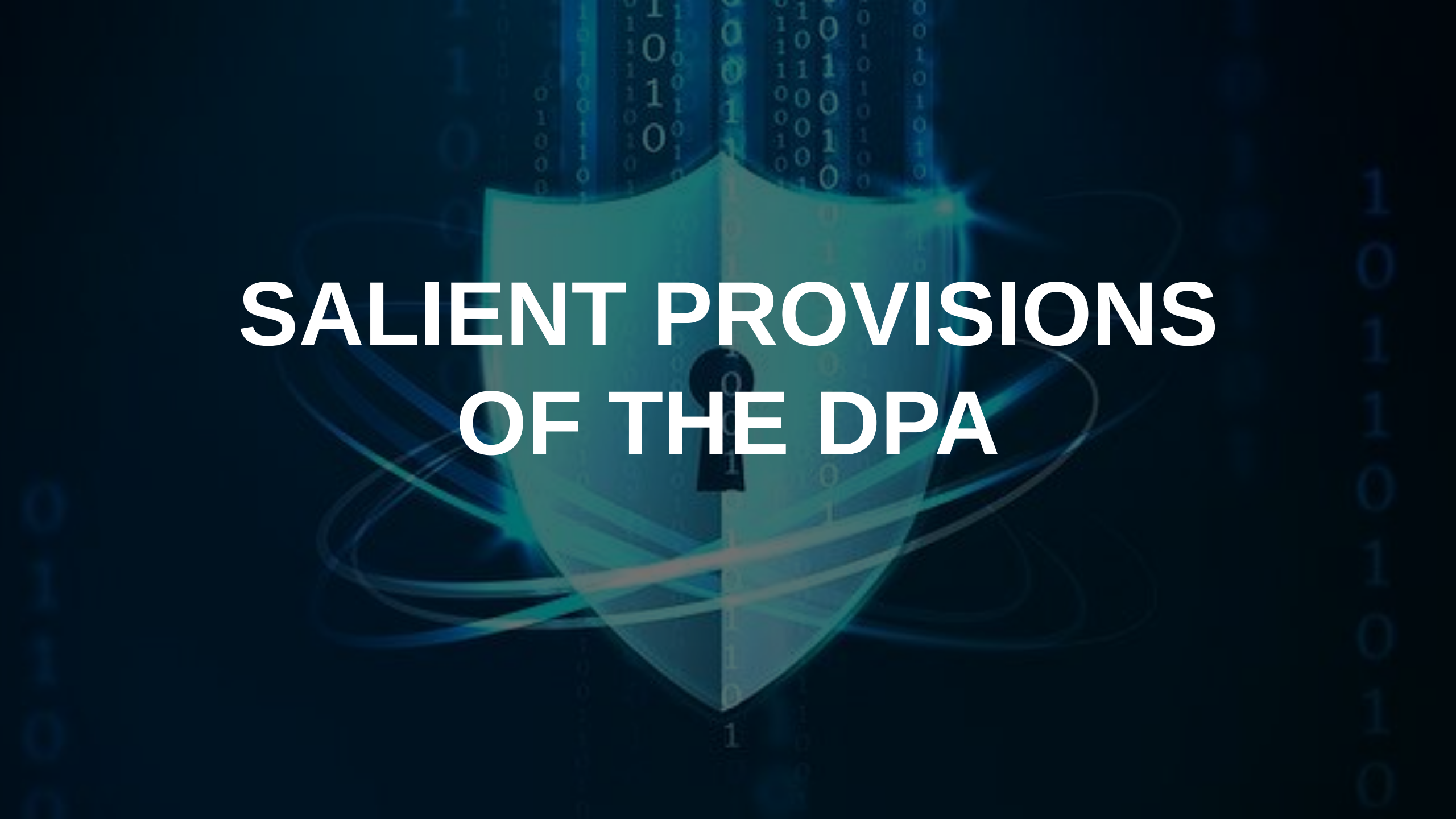
- In Kenya, the DPA was assented to by the President on 8th November 2019 and commenced on 25th November 2019.

- It gives effect to Article 31(c) and (d) of the Constitution and is aimed to operate in two ways:

✓ giving individuals certain rights whilst requiring responsibility from those who record and use personal information.

- More significantly, the Data Commissioner was appointed on 12th November 2020 thus setting in motion the operationalization of not only the ODPC but also the DPA.





SALIENT PROVISIONS OF THE DPA

Salient provisions of the DPA

Understanding the Terminology

- The DPA defines "**Data**" as information which-
    a) Is processed by means of equipment operating automatically in response to instructions given for that purpose;
    b) Is recorded with the intention that it should be processed by means of such equipment;
    c) Is recorded as part of a relevant filing system; or
    d) Where it does not fall under (a) to (c), forms part of a relevant record; or
    e) Recorded information held by a public entity.
- The definition is wide and covers both electronically generated and manually collected data as long as the same forms part of a relevant record or is information held by a public entity.
- **"Personal data"** is any information relating to an identified or identifiable individual (***data subject***).
- **"Processing"** is also widely defined to include a host of operations such as collection, storage, retrieval, disclosure of alignment, whether conducted by automated or manual processes. This is widely defined to cover all conceivable operation or sets of operations.

Salient provisions of the DPA – Contd.

- **“Data controller”** is a natural or legal person which determines the purpose and means of processing personal data while a “data processor” is a natural or legal person which processes personal data for the data controller.

Explanation

- The **data controller** determines the **purposes** for which and the **means** by which personal data is processed e.g. if a company/organisation decides ‘why’ and ‘how’ the personal data should be processed it is the data controller. Employees processing personal data within the organisation do so to fulfil the organisation’s tasks as data controller.
- The **data processor** processes personal data only **on behalf of the controller**. The data processor could be a third party external to the company/organisation. However, in the case of groups of undertakings, one undertaking may act as processor for another undertaking. A typical activity of processors is offering IT solutions, including cloud storage.
- It is possible to be both a data controller and a data processor at the same time e.g. an internal accounting department of an organization that processes pay roll information in respect of its employees every month.

THE OBJECT & PURPOSE

The fundamentals

- Section 3 sets out the objects and purpose of the Act as follows:
    a) To regulate the processing of personal data;
    b) To ensure that the processing of personal data of a data subject is guided by the data protection principles;
    c) To protect the privacy of individuals;
    d) To establish the legal and institutional mechanism to protect personal data; and
    e) To provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with the Act.
- The objects and purpose of the Act hark back to Article 31 (c) and (d) of the Constitution and place an emphasis on the privacy of the personal data relating to individuals.
- There is an emphasis for processing of personal data in line with data protection principles as set out under section 25 of the Act signifying their importance to the DPA as a whole.
- There is also an emphasis on processing as per the provisions of the Act and forms the basis for enforcement provisions which appear at Part VIII of the Act.

INSTITUTIONAL STRUCTURES AND REGISTRATION FORMALITIES

Institutional structures and registration formalities

- **Section 5** of the DPA establishes the Office of the Data Protection Commissioner ("**ODPC**").
- ODPC comprise of the Data Commissioner & other staff appointed by the Data Commissioner.
- Functions & Powers of Data Commissioner include:-

i. Oversee the implementation of and responsible of the enforcement of the DPA;

ii. Establish & maintain a register of data controllers and data processors;

iii. Exercise oversight on data processing operations;

iv. Receive and investigate complaints on infringements of rights under the Act & impose administrative fines for failures to comply with the Act…. **etc**

Institutional structures and registration formalities – Contd.

- Section 18 requires data controllers and data processors to register with the Office of the Data Commissioner.
- Sub-section (2) - the Data Commissioner shall prescribe thresholds for registration based *inter-alia* on the nature of the industry, the volume of the data processed and whether any sensitive personal data is being processed.
- The Application for registration by a data controller or data processor is made under Section 19 & must provide the particulars specified under sub section (2).
- Sections 20 and 21 provide for duration of & renewal of registration certificate and the maintenance of a register of the registered data controllers and data processors.
- Section 23 bestows the power to carry out periodic audits of the processes and systems of controllers & processors on the Data Commissioner in order to ensure compliance with the provisions of the Act.
- The powers bestowed on the Data Commissioner to carry out audits are wide and there is no limitation provided within the Act on the basis for exercise of the said powers.

Core data protection principles

- Section 25 of the Act is important as it sets out the following data protection principles which provide that data controllers and processors must ensure that data is-
    a) Processed in accordance with the right to privacy of the data subject;
    b) Processed lawfully, fairly and in a transparent manner in relation to any data subject;
    c) Collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
    d) Adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
    e) Collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
    f) Accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
    g) Kept in a form which identifies the data subjects for no longer than is necessary for which it was collected; and
    h) Not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

Correlation to EUGDPR

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

Rights of the data subject

- Section 26 of the DPA sets out the rights of the Data Subject-
  - a) to be informed of the use to which their personal data is to be put;
  - b) to access their personal data;
  - c) to object to the processing of all or part of their personal data;
  - d) to correction of false or misleading data; and
  - e) to deletion of false or misleading data about them.
- The rights set out in 26 (a) to (c) out lay an emphasis on **consent** and transparency with regard processing of personal data while (c) and (d) lay emphasis on accuracy- **the Transparency and Accuracy Principles**.
- Section 30 1 (a) provides for lawful processing with the consent of the data subject while section 30 (1) (b) (i) to (viii) provides for lawful processing without consent in certain instances, the most notable of which are; where it is for the performance of a contract to which the data subject is a party, exercise of functions which are of a public nature, compliance with a legal obligation to which the data controller is subject or for scientific research, historical, journalistic and statistical purposes.

Rights of the data subject – Contd.

- Under Section 32 the data controller of data processor has the burden of proof for establishing a data subject's consent to the processing of their data for specified purposes- **the Accountability Principle**.
- Section 34 restricts the processing of personal data where its accuracy is contested by the data subject, the data is no longer required for the purpose for which it is collected or where the data subject has objected to the processing. Where processing of personal data is restricted it can only be used without consent for the defence or establishment of a valid legal claim- **the Accuracy and Purpose Limitation Principles**.
- Section 39 provides that the a data controller or data processor shall retain personal data for only as long as may be reasonably necessary to satisfy the purpose for which it was collected unless the storage is required or authorized by law or for a lawful purpose- **the Storage Limitation Principle**.
- Section 40 provides for rectification of false, inaccurate, outdated or misleading personal data.
- Section 41 places an obligation on a data controller or data processor to implement appropriate technical and organisational measures in compliance with data protection principles- **The integrity and Confidentiality Principle**.

Elements of consent

i. Choice: freely given i.e

- data subject should be given a genuine choice &
- control over use of their data.

ii. Specificity:

- a specific lawful processing purpose
- communicated clearly.

iii. Express: a direct, clear oral or written statement from the data subject. i.e. No implied consents

iv. Affirmative Action: a deliberate and specific action agreeing or "*opting–in*" to processing

e.g. ticking a box on a website.


OTHER
PROVISIONS

Other provisions

Grounds for Processing of Sensitive Personal Data

- **Ss. 44-47** of the Act outline the grounds for processing of sensitive personal data by:
  - Prohibiting the processing unless section 25 of the Act applies to that processing.
  - Specifying the permitted grounds for processing sensitive personal data.
  - Restricting the processing of Personal data relating to health.

Transfer of Data out of Kenya

Section 48 sets conditions for transfer of data out of Kenya.

Section 49 provides for the following pre-requisites to such transfer;

- Provide proof of safeguarding the personal data
- Obtain consent for the transfer
- Show the necessity for the transfer of the data

Other provisions – Contd.

Exemptions

- Ss. 51 & 52 general **exemptions** to processing of data:
    i. disclosure is required by any written law or a court order;
    ii. Necessary for national security or public interest;
    iii. relates purely to a personal or household activities;
    iv. undertaken by a person for journalistic, literal and artistic purposes
    v. Compliance is incompatible with “the special purposes”
- Data commissioner may prescribe other exemptions

Other provisions – Contd.

Enforcement

- The Enforcement Provisions are set out under Part VIII of the Act.

  - Lodge a complaint orally or in writing with the Data Commissioner;
  - Investigation of the complaint to be carried out within 90 days;
  - Data Commissioner has powers during investigation to summon & order production of documents, written statements, etc
  - Data Commissioner has powers to issue enforcement notices
  - Non-compliance of an enforcement notice constitutes a criminal offence i.e. exposure to a fine (≤ KES 5m) or imprisonment (≤ 2 years) or both
  - Data Commissioner has powers to issue penalty notices
  - Maximum penalty – KES 5m
  - Other remedies – compensation and preservation order.

Other provisions – Contd.

Miscellaneous

- **Section 71** delegates powers to make regulations to the Cabinet Secretary.
- **Section 72** prescribes offences for unlawful disclosure of personal data.
- **Section 73** prescribes a general penalty where no specific penalty is provided (fine ≤ KES 3m or imprisonment for a term ≤10 years or both)
- **Section 74** empowers Data Commissioner to issue guidelines or codes of practise for data controllers, processors & data protection offices (e.g. the Guidance Notes on Consent and Data Protection Impact Assessment)

What next?

- Undertaking a systems and personal data audit
- Development of a Data Protection Policy
- Appointment of the Data Protection Officer (can be shared between related entities)
- Registration with the Data Commissioner
- Establishment of suitable organizational and technical measures to prevent potential breaches, unauthorized access or illegal processing (data protection by design and default).
- Identify third party data processors contracted by the company and review contracts with them to ensure compliance with the DPA
- Carrying out a Data Protect Impact Assessment (DPIA) to identify potential gaps and to determine how to address the same


JURISPRUDENCE

WM Morrison Supermarkets Plc v Various Claimants [2020] UKSC 12

- Facts of the Case:
  - Appellant's employee published his colleagues' personal data on the internet as an act of vengeance against his employer. The employees sued the appellant for misuse of personal information (under the UK DPA) and breach of the duty of confidence (common law).

- Issues and Outcome:
  - Whether the Appellant is vicariously liable for its employee's conduct - *No. He was on a frolic of his own.*
  - Whether the DPA excludes the imposition of vicarious liability for statutory torts committed by an employee data controller under the DPA – *No.*
  - Whether the DPA excludes the imposition of vicarious liability for misuse of private information and breach of confidence – *No.*

HRH the Duchess of Sussex v Associated Newspapers Limited [2020] EWHC 1058 (Ch), 2020 WL 02089151

- Background:
  - Judgment on a Pre-Trial Application to strike out certain particulars of the Claim for misuse of private information and breach of data protection rights.
- Relevant Issue:
  - Whether the allegation that the Defendant acted dishonestly and in bad faith are irrelevant in law, or inadequately particularised.
- Relevant Finding:
  - Dishonesty, malice, or bad faith are irrelevant to liability for misuse of private information. Motive is not relevant.
- A data subject aggrieved by the acts of a data processor or controller who has contravened the DPA may seek compensation in the form of damages for financial loss and distress (S.65 DPA).

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González

- Background:
  - Reference from the National High Court of Spain to the ECJ for a preliminary ruling on Directive 95/46.

- The principles in Section 25 of Kenya's DPA mirror those in this Directive.

- Interpretation with regards to Internet Search Engines:
  - Data controllers to ensure data is: processed lawfully and fairly, collected for specified and legitimate purposes, accurate, relevant, and kept up to date. If not, data controller to ensure it is deleted.
  - The "right to be forgotten", depending on the circumstances of the case, may override the economic interest of the search engine owner as well as the general public in having access to that information.


?
Q
&
&
A
!

Disclaimer

This presentation is of a general nature and solely for information purposes. The information herein counts as expert opinion but not professional advice. The presentation is not intended to address the circumstances of any particular individual or entity. While the information is accurate as at the date hereof, there can be no guarantee that the information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice and after a thorough examination of the particular situation.

If you require specific advice on this matter, please write to us through legal@oraro.co.ke.

ORARO & COMPANY
ADVOCATES

ACK Garden Annex, 6th floor, 1st Ngong Avenue, P.O Box 51236-00200, Nairobi, Kenya
E: legal@oraro.co.ke
T: +254 709 250 000

Thank you