Data Protection in Kenya

The Institute of
Internal Auditors

Mercy Wanjau, MBS

May 10, 2022

IIA Kenya Annual Seminar

The auditor as a compliance partner

- Compliance, Legal, Privacy, Risk management, IT security + Internal Audit

- How?

- engaging early and often in the data protection lifecycle
- advising on the status of current controls
- performing privacy risk assessments and performing detailed testing of systems
- unpack the complexities of DP & drive a proactive approach toward compliance while also safely leveraging data to its full value

Where did the concept come from?

1890 - the "right to be left alone” (USA)

1948 – UDHR is adopted, including the 12th fundamental right, i.e. the Right to Privacy.

1950 - The EU Convention on Human Rights (Europe)

1967 - The Freedom of Information Act (FOIA) gives everyone the right to request access to documents from state agencies. (USA)

1980 - OECD issues guidelines on data protection, reflecting the increasing use of computers to process business transactions

1995 - The European Data Protection Directive is created, reflecting technological advances and introducing new terms including processing, sensitive personal data and consent, among others.

Down the memory path

Our own information is being weaponized against us with great efficiency

2014 - A ruling by the Court of Justice of the EU gives rise to a concept known as “the right to be forgotten”.

2016 -The General Data Protection Regulation (GDPR) is approved by the EU parliament after 4 years of discussions.

2018 - GDPR is enforced, replacing the Data Protection Act.

TODAY …….

Responsible management of personal data through mature IT governance, transparent processes and modern applications.

Bringing it home …

Vitu kwa ground….

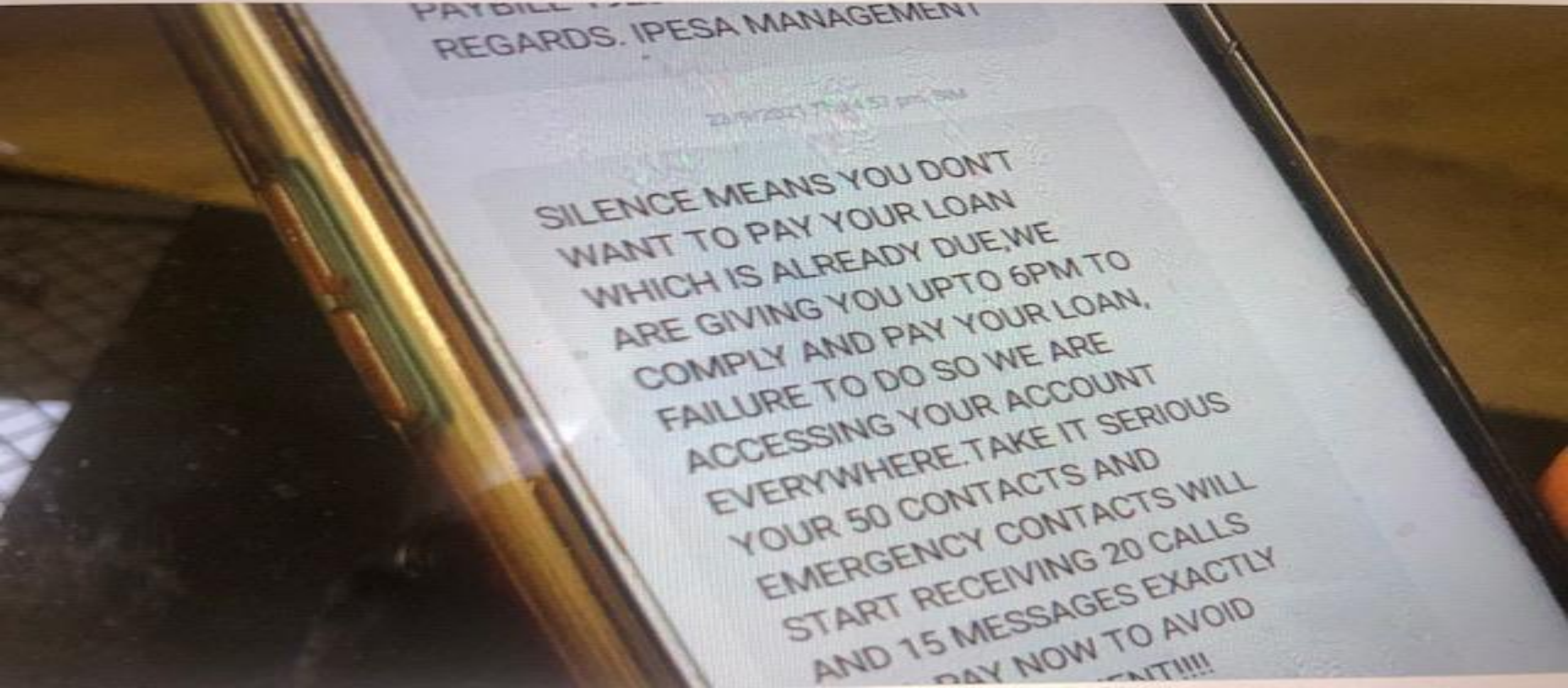
The Constitution of Kenya, 2010 guarantees the right to privacy as a fundamental right.

Article 31 of the Constitution states, "every person has the right to privacy, which includes the right not to have— (a) their person, home or property searched; (b) their possessions seized; (c) information relating to their family or private affairs unnecessarily required or revealed; or (d) the privacy of their communications infringed."

Article 35 (2) ensures the right of every person to the correction or deletion of untrue or misleading information that affects the person.

The perception of privacy through the lens of cultural norms – an 'untrodden path'

Looks familiar?



PAYBILL

REGARDS. IPESA MANAGEMENT

23/9/2021 [illegible]:53 pm, SIM

SILENCE MEANS YOU DON'T WANT TO PAY YOUR LOAN WHICH IS ALREADY DUE,WE ARE GIVING YOU UPTO 6PM TO COMPLY AND PAY YOUR LOAN, FAILURE TO DO SO WE ARE ACCESSING YOUR ACCOUNT EVERYWHERE.TAKE IT SERIOUS YOUR 50 CONTACTS AND EMERGENCY CONTACTS WILL START RECEIVING 20 CALLS AND 15 MESSAGES EXACTLY

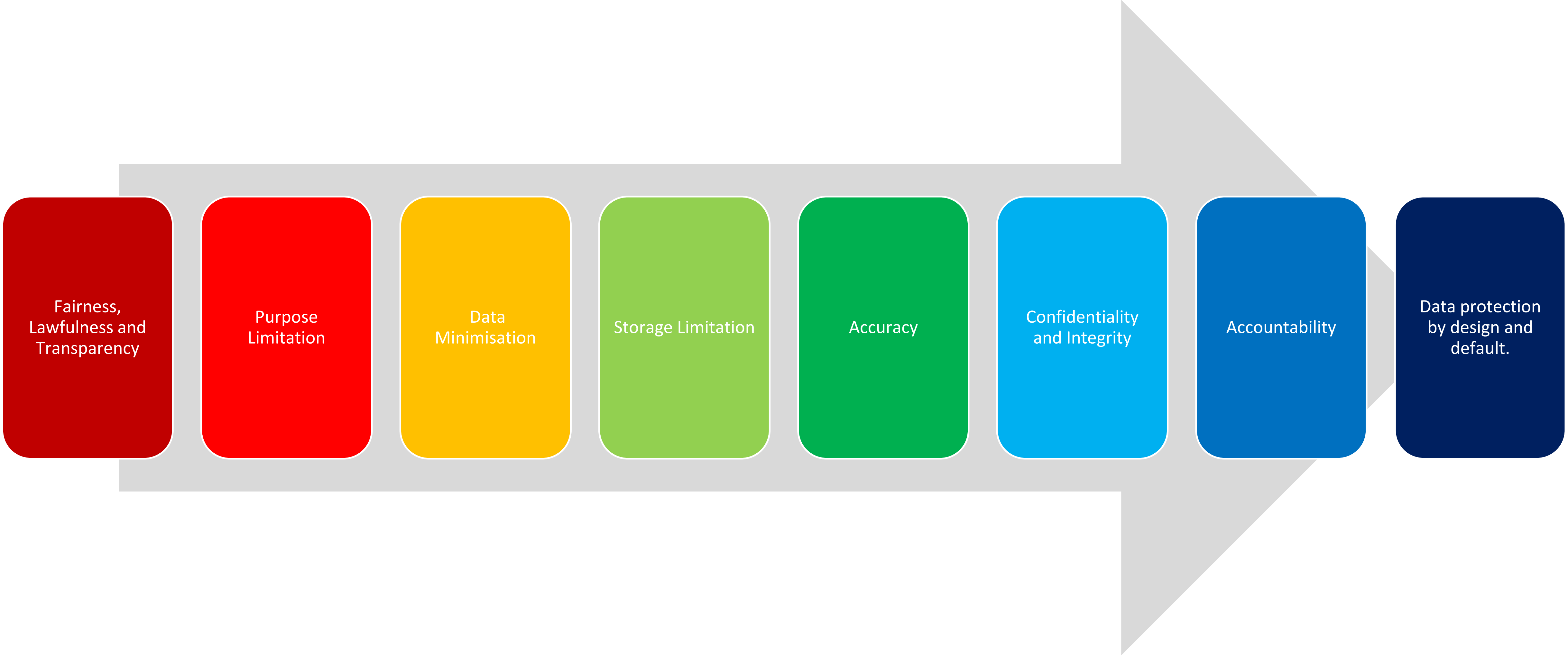
PAY NOW TO AVOID

ENT!!!!

Objective of the DP framework

- To enhance effective application of data protection laws
- To comply with international good practice and set out practices and procedures in administering the laws
- To ensure effective protection and management of personal data
- To establish the institutional framework
- To offer clarity on processing of personal data
- Protection of personal data relating to children.
- Protect the country from the risk of personal data breaches
- Provide an enabling trade environment through cross-border transfer of data.

Principles governing data processing



Fairness, Lawfulness and Transparency

Purpose Limitation

Data Minimisation

Storage Limitation

Accuracy

Confidentiality and Integrity

Accountability

Data protection by design and default.

How much data are you generating right now?

1	Name, family details inc. names of children, spouse (s)	15	Photo
2	Email address	16	IP addresses
3	Mobile device numbers, IMEI	17	Bank details / Loyalty prog. details
4	Geolocation records	18	Gender, race
5	Social media details	19	Site user names
6	Phone numbers	20	Passport / ID / Social security numbers
7	Dates of birth	21	Arrival & departure info
8	Reservation dates	22	Communication preferences
9	Credit card numbers & expiry dates	23	Genomic information
10	Login credentials eg. User names & passwords	24	Health data
11	Financial information	25	Consumer behaviour - spending how much & on what
12	Residential address	26	Frequent contacts

Data Protection concerns for organizations

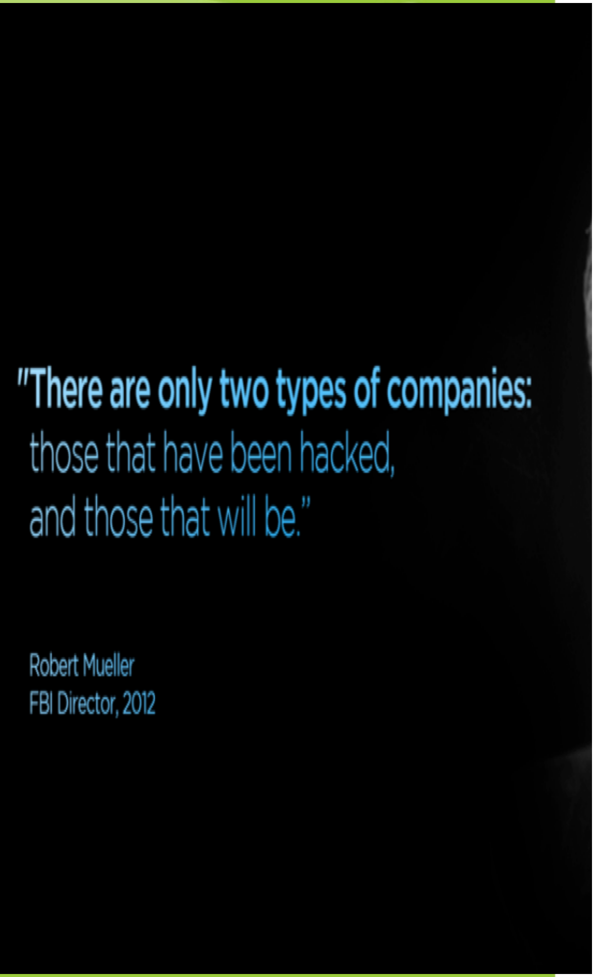
- Digital transformation has increased the supply of data
- Data breaches will only increase as attackers exploit the data-dependencies of daily life
- Impact of data breaches affects hundreds of millions or even billions of people at a time
- Personal Identifiable Information (PII) is a precious commodity
- It is overwhelming to handle millions and possibly even billions of data records
- It gets complicated when data transfer is across jurisdictions and contains sensitive data

Compliance challenges for organizations

- Employee data
- IoT
- BYoD
- Remote working

Data protection is a set of strategies and is vital for any organisation that collects, handles, or stores personal data. A successful strategy can help prevent data loss, theft, or corruption and can help minimise damage caused in the event of a breach. Operational controls are procedures and rules implemented to protect systems, applications, and the organisation as a whole by addressing the gaps across the information lifecycle.

Major data breaches



"There are only two types of companies: those that have been hacked, and those that will be."

Robert Mueller
FBI Director, 2012

1. **Yahoo** August 2013 **Impact:** 3 billion accounts Affected price of Verizon deal
2. **Alibaba** November 2019 **Impact:** 1.1 billion pieces of user data 3 years imprisonment
3. LinkedIn June 2021 **Impact:**700m users
4. **Sina Weibo** March 2020 **Impact:** 538 million users. Database was sold on the dark web for $250
5. **Marriot International** September 2018 **Impact:** 500m hotel guests Exposure of sensitive data. Fined £18.4m (reduced from £99 m) by UK ICO
6. **Adult Friend Finder** October 2016 **Impact:** 412.2 million accounts Due to sensitive nature of the services offered ,potential to be particularly damming for victims

Going forward…

Date Protection compliance

Tips for protecting your organization's data

- Appreciate roles & responsibilities of your org. under the DP framework
- Introduce DP in the boardroom as a substantive regulatory agenda
- Include DP in the risk ecosystem
- Undertake assessment of gaps across business processes
- Implement a DP compliance plan to close the gaps
- Encrypt data
- Communicate data securely
- Use access controls and firewalls.
- Use external service providers carefully
- Keep some data off the network

> “the weakest link in a company’s security chain is typically people”

Data Protection / Privacy Principles	Clinical Data Management	Compensation and benefits	Consumer Complaints/Enquiries/Feedba	Consumer PR	Consumer Refund Management	Consumer Resolution Process	Consumer Respondent Profiling	Consumer Survey	Contest	Corp Secretarial Services	Corp Tax Submission	Credit Application	Customer Account Creation	Customer Complaints	Customer Services	Customer acquisition	Customer relationship management reco	Division Incentive Trip	Document Processing	E-Commerce Contest	Employee Claims	Facility Management	Freelancer Payment	Grant Audit	HR Re
	Collection and Usage Repository																								
Lawfulness - Consent	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	⬛	⬛	🟩	🟩	🟩	🟩	🟩	-	🟥	⬛	-	🟥	⬛	🟩	🟩
Transparency - Notice	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟥	🟥	🟩	⬛	⬛	🟥	🟥	🟥	🟥	🟥	-	🟥	🟥	-	🟥	🟥	🟩	🟩
Purpose Limitation	🟩	🟥	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟩	-	🟩	🟥	-	🟩	🟥	🟩	🟩
Data Minimisation	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	🟥	🟥	🟥	🟩	-	🟥	🟥	-	🟥	🟥	🟥	🟩
Data Quality / Accuracy	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥	⬛	-	🟥	🟥	-	🟥	🟩	🟩	⬛
	Disclosure Repository																								
Disclosure / Transfer - Contract	🟩	🟩	🟩	🟩	🟩	⬛	🟥	🟩	🟩	🟥	🟩	🟩	⬛	🟥	🟩	🟥	🟩	🟩	🟥	🟥	🟩	🟥	🟥	-	-
	Storage Repository																								
Storage Limitation - Retention Period	🟥	🟩	🟥	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	🟥	🟩	-	🟥	🟥	🟥	🟩	🟥	🟥	🟥	🟥	🟥	-	🟥
Storage Limitation - Retention Policy	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	-	🟥	🟥	🟥	🟩	🟥	🟩	🟥	🟥	🟩	-	🟥
Confidentiality & Integrity - Security / Encryption	🟩	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟥	-	🟥	🟥	🟥	🟩	🟥	🟥	🟩	🟥	🟥	-	🟥
Confidentiality & Integrity - Access Control	🟩	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟥	🟥	🟩	🟩	⬛	-	🟥	🟥	🟩	🟩	🟩	🟥	🟩	🟥	🟥	-	🟥

A call for urgency

- GoK – emphasis on adoption of technology and innovation to leapfrog her economy and promote solutions for meeting development challenges facing Kenya and Africa at large.

  - The National ICT Policy

  - Kenya's Digital Economy Blueprint for Africa, 2019

  - The Draft Digital Economy Strategy for Kenya which is a five-year roadmap to operationalise the Digital Economy Blueprint.

"Before I write my name on the board, I'll need to know how you're planning to use that data."

Thank you!

Mercy Wanjau, MBS

Director, Legal Services @ Communications Authority of Kenya

wanjau@ca.go.ke