



Kenya Data Protection Act Quick Guide

2021

Introduction

Overview

Kenya has promulgated a Data Protection Act....

The Data Protection Bill that has been a subject of discussion for years, was passed into law on 8 November 2019 when the president assented to it. The Data protection Bill 2019, follows the path taken by the European Union in enacting the General Data Protection Regulation (GDPR) in May 2018 and makes Kenya the third country in East Africa to have legislation dedicated to data protection.

This law was expedited following concerns raised over the *Huduma Namba* registration exercise, with those opposed to the process raising concern about the safety of citizen's personal data collected by the Government.

Purpose of the Act

The Act seeks to:

- give effect to Article 31(c) and (d) of the Constitution that contain the right to privacy;
- establishment of the Office of the Data Commissioner;
- regulate the processing of personal data,
- provide for the rights of data 'subjects'; and
- obligations of data 'controllers' (Person who determines the purpose and means of processing of personal data) and 'processors' (Person who processes personal data on behalf of the data controller).

Data Protection Principles

The Act requires Data Controllers and Processors to **process data lawfully; minimise collection of data; restricts further processing of data; requires data controllers and processors to ensure data quality;** and that **they establish and maintain security safeguards to protect personal data.**

Registration of Data Controllers and Processors

The Act requires that any person who acts as a data controller or data processor must be registered with the Data Commissioner. Therefore, once the office of the Data Commissioner is established, organisations meeting the definition of a controller or processor will need to register as such, and renew their registration every 3 years.

Transfer of Personal Data Outside Kenya

- Every data controller or data processor is required to ensure the storage, on a **server or data centre located in Kenya**, of at least one serving copy of personal data to which the Act applies.
- Cross-border processing of sensitive personal data is prohibited and only allowed when certain conditions are met or under certain circumstances specified in the Act (Part IV – 48 – 50).
- A data controller or data processor may transfer personal data to another country where—
 - i. the data controller or data processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of the personal data;
 - ii. the data subject has given explicit consent to the proposed transfer, after having been informed of the possible risks of the transfer such as the absence of appropriate security safeguards;
 - iii. the transfer is necessary for performance of a contract.

Exemptions

The processing of personal data is exempt from the provisions of the Data protection Act if—

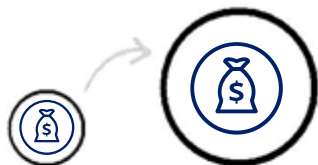
- i. exemption is necessary for national security or public order;
- ii. disclosure is required by or under any a written law or by an order of the court e.g. Anti Money Laundering (AML) Laws;
- iii. the prevention or detection of crime e.g. AML/CFT laws;
- iv. the apprehension or prosecution of an offender; or
- v. the assessment or collection of a tax or duty or an imposition of a similar nature.

Recent Developments

- i. **Recruitment of the Data Commissioner** to head the Office of the Data Protection Commissioner in October 2020 and subsequent vetting by parliament, appointment and swearing in of Ms. Immaculate Kassait.
- ii. 15 January 2021: Appointment of 14-member task force chaired by Immaculate Kassait to review the Act, identify gaps or inconsistencies in the law, propose any new policy, legal and institutional framework that may be needed to implement the Act, develop the Data Protection (General) Regulations and train stakeholders and the public on the said regulations.

The Big Picture

Key Elements of the Data Protection Act



PENALTIES FOR NON COMPLIANCE

Infringement of provisions of the Kenya Data Protection Act (DPA) will attract a penalty of not more than KES 5 million or, in the case of an undertaking, not more than 1% of its annual turnover of the preceding financial year, whichever is lower. Individuals will be liable to a fine not exceeding three million shillings or to an imprisonment term not exceeding ten years, or to both.



INCREASED TERRITORIAL SCOPE

DPA will apply to all companies processing the personal data of data subjects residing in Kenya, regardless of the company's location.



EXPLICIT AND RETRACTABLE CONSENT FROM DATA SUBJECTS

Must be provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.



DATA SUBJECT RIGHTS

Data subjects can request confirmation whether or not their personal data is being processed, where and for what purpose. Additionally, data subjects can request to be forgotten, which entails the removal of all the data related to the data subject.



BREACH NOTIFICATION WITHIN 72 HOURS

Notify the Data Commissioner within seventy-two hours of becoming aware of a breach and to the data subject in writing within a reasonably practical period.



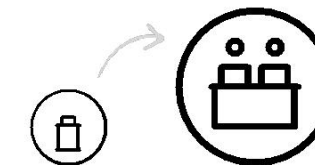
PRIVACY BY DESIGN

Now a legal requirement for the consideration and inclusion of data protection from the onset of the designing of systems, rather than a retrospective addition.



DATA INVENTORY

Organizations must maintain a record of processing activities under its responsibility—or, in short, they must keep an inventory of all personal data processed. The inventory must include the multiple types of information, such as the purpose of the processing.



MANDATORY DATA PROTECTION OFFICERS

Depending on the type of personal data and intensity of processing activities, an organisation may be required to appoint a Data Protection Officer to facilitate the need to demonstrate compliance to the Act.

Impacts to Organisations

The Data Protection Act impacts many areas of an organisation, mainly: **legal and compliance**, **technology**, and **data**.

Legal & Compliance





The Data Protection Act (DPA) introduces new requirements and challenges for legal and compliance functions. Many organisations will require a Data Protection Officer (DPO) who will have a key role in ensuring compliance. If the DPA is not complied with, organisations will face the heaviest fines yet – up to 2% of previous year turnover. A renewed emphasis on organisational accountability will demand proactive robust privacy governance. This will require organisations to review how they write privacy policies to make these easier to understand, and enforce compliance.

-  Chief Risk Officer
-  Chief Information Security Officer
-  Compliance Officer
-  Chief Legal Officer

Technology



New DPA requirements will mean changes to the ways in which technologies are designed and managed. Documented Data Protection Impact Assessments will be required to deploy major new systems and technologies that are likely to result in high risk to the rights and freedoms of data subjects. Security breaches will have to be notified to regulators within 72 hours, meaning implementation of new or enhanced data security approaches and incident response procedures. The concept of Privacy now becomes enshrined in law, with the Privacy Impact Assessment expected to become commonplace across organisations over the next few years. And organisations will be expected to look more into data masking, pseudonymisation and encryption.

-  Chief Technology Officer/Chief Information Officer
-  Chief Information Security Officer

Data



Individuals and teams tasked with data and information management will be challenged to provide clearer oversight on data storage, journeys, and lineage. Having a better grasp of what data is collected and where it is stored will make it easier to comply with (new) data subject rights – rights to have data deleted and to have it ported to other organisations. This will also have an impact on Third Party vendors that an organization works with.

-  Chief Data Officer
-  Chief Operating Officer

Impacts – Legal and Compliance

Chief Risk & Compliance Officers, Legal Officers, Privacy Officers and Data Protection Officers: Your privacy strategies, resourcing, and organisational controls will need to be revised. Boardrooms will need to be engaged more than ever before.

1

A Revolution in Enforcement

Fines up to 1% of prior year annual turnover

Serious non-compliance could result in fines of up to five million shillings, or in the case of an undertaking, up to 1% of its annual turnover of the preceding financial year, whichever is lower. Individuals could face fines not exceeding three million shillings or an imprisonment term not exceeding ten years, or both.

Enforcement action will **extend to other countries** where analysis on Kenya citizens is performed. But how will this play out in practice?

2

Accountability

Proactive approach

There will be significant new requirements around **maintenance of audit trails and data journeys**. The focus is on organisations having a **more proactive**,

comprehensive view of their data and being able to demonstrate they are **compliant** with the Data Protection Act requirements.

3

Data Protection Officers

Market heats up for independent specialists

Organisations processing personal data on a large scale will now be required to **appoint an independent, adequately qualified Data Protection Officer**. This will present a challenge for many medium to large organisations, as individuals

with sought-after skills and experience are currently in short supply.

4

Privacy Notices and Consent

Clarity and education is key

Organisations should now consider carefully how they construct their **public-facing privacy policies** to provide more detailed information. However, it will no longer be good enough to hide behind pages of legalese. In addition, the Data Protection Act will retain the **notion**

of **consent as one of the conditions for lawful processing**, with organisations required to obtain 'freely given, specific, informed and unambiguous' consent, while being able to demonstrate these criteria have been met.



Impacts – Technology

Chief Information Officers, Chief Technology Officers and Chief Information Security Officers: Your approach towards the use of technology to enable information security and other compliance initiatives will need to be reconsidered, refocused and repurposed with costs potentially rising.

1

Breach Reporting

Breach reporting within 72 hours of detection

Significant data **breaches** will now have to be **reported** to regulators and in some circumstances also to the individuals impacted. This means organisations will have to urgently revise their

incident management procedures and consider processes for regularly testing, assessing and evaluating their end to end incident management processes.

2

Online Profiling

Profiling & automatic decision-making becomes a loaded topic

Individuals will have new rights to **opt out of** and **object to online profiling** and **tracking**, significantly impacting direct-to-consumer businesses who rely on such techniques to better understand their customers.

Automatic decision-making on issue affecting the privacy or dignity of a data subject is also now regulated. This applies not just to websites/platforms, but also to other digital assets, such as mobile apps, wearable devices, and emerging technologies.

3

Encryption

Encryption as means of providing immunity?

The Data Protection Act formally recognises the privacy benefits of encryption. In case of a data breach, where **encryption safeguard** was adopted, the law **exempts** the data controller or processor from notifying affected data subjects. However,

this does not mean that organisations can afford to be complacent, and the exemption may not apply when weak encryption has been used. Given the potential fines, organisations will have to further increase their focus on a robust information and cyber security regime.

4

Privacy-by-Design and Privacy-by-Default

Recognised best practice becomes law

The concept of Privacy by Design and by Default (**PbD**) is nothing new, but now it is **enshrined** in the Data Protection Act. Organisations need to build a mind set that has privacy at the forefront of the design, build and deployment of new

Technologies (by design) and in their business-as-usual operations (by default). One demonstration of PbD is **Data Protection Impact Assessments (DPIA)**, which is now required to be undertaken for new uses of personal data where the risk to individuals is high.

Impacts – Data

Chief Data Officers, Data Stewards, Chief Marketing Officers, and Digital Leads: Your information management activities have always supported privacy initiatives, but under the Data Protection Act, new activities are required which specifically link to compliance demands.

1

Data Inventories

Identifying and tracking data

Organisations will have to take steps to demonstrate they **know what** data they **hold**, **where** it is **stored**, and **who** it is **shared with**, by creating and maintaining an inventory of data processing

activities. Data leads will have to work closely with privacy colleagues to ensure all necessary bases are covered. A thorough system for maintaining inventories needs to be implemented.

2

Right to Data Portability

A new right to request standardised copies of data

A new right to 'data portability' means that individuals are entitled to request **copies of their data in a readable and standardised format**. The interpretation of this requirement is debatable,

but taken broadly the challenges could be numerous – amongst them achieving clarity on which data needs to be provided, extracting data efficiently, and providing data in an industry-standardised form.

3

Right to be Forgotten

A stronger right for consumers to request deletion of their data

A new 'right to be forgotten' is further evidence of the consumer being in the driving seat when it comes to use of their data. Depending on regulatory interpretation, organisations may need to

perform **wholesale reviews** of processes, system architecture, and third party data access controls. In addition, **archive media** may also need to be reviewed and data deleted.

4

Definitions of Data

The concept of pseudonymisation of data

The Data Protection Act expressly recognises the concept of pseudonymisation of data and places emphasis on **data classification and governance**. But it remains unclear if and when certain

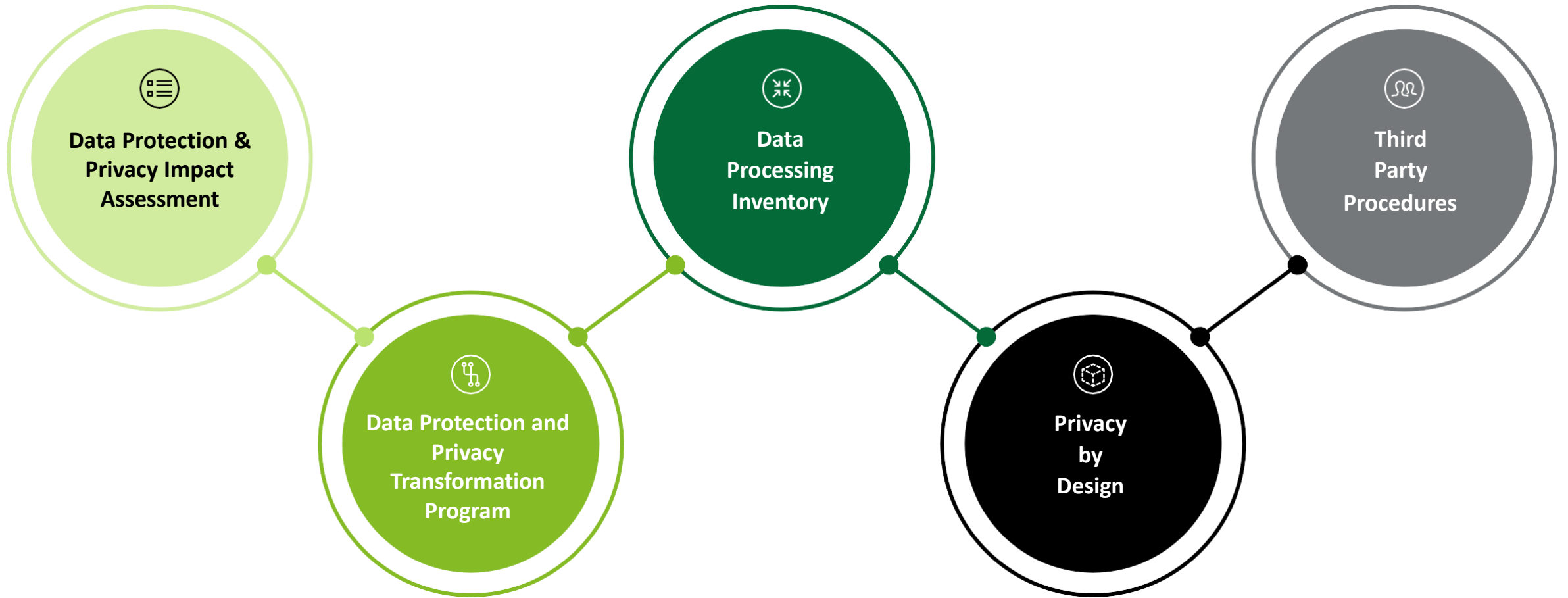
data will be classed as personal data and subject to requirements.



Deloitte's Approach to the Data Protection Act

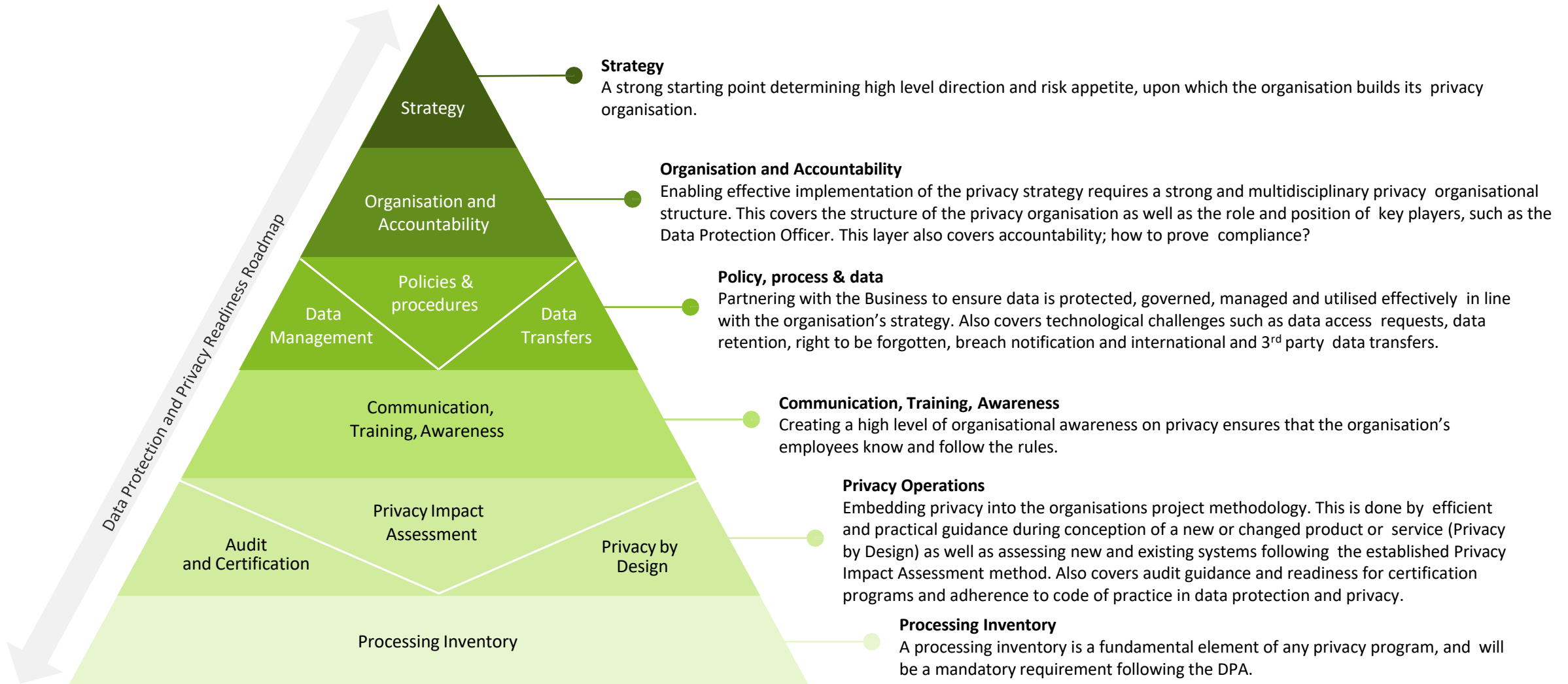
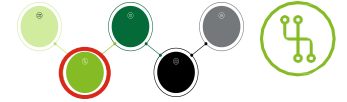
Approach – Actions to take

Actions to take to prepare for the Data Protection Act (DPA) and other Data Protection Regulations



Approach - Actions to take to prepare for the Data Privacy Regulations

Based on a comprehensive DPA readiness roadmap, a tailored transformation program helps organisations prepare in the optimal way for the Data Protection Regulations



Contacts



Urvi Patel
Partner, Risk Advisory

Tel: +254 (0) 711 584 007
Email: upatel@deloitte.co.ke



Julie Nyang'aya
Partner, Risk Advisory

Tel: :+254 (0) 720 111 888
Email : julnyangaya@deloitte.co.ke



Rakesh Ravindran
Manager, Risk Advisory

Tel: :+254 (0) 790 710 311
Email : rravindran@deloitte.co.ke



Samuel Njoroge
Manager, Risk Advisory

Tel: +254 (0) 710 546 333
Email : snjoroge@deloitte.co.ke



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients’ most complex business challenges. To learn more about how Deloitte’s approximately 334,800 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.