DATA PROTECTION REGULATIONS

presentation on:

The Data Protection General Regulations, 2021

By:

Taskforce on the development of the Data Protection General Regulations

April, 2021

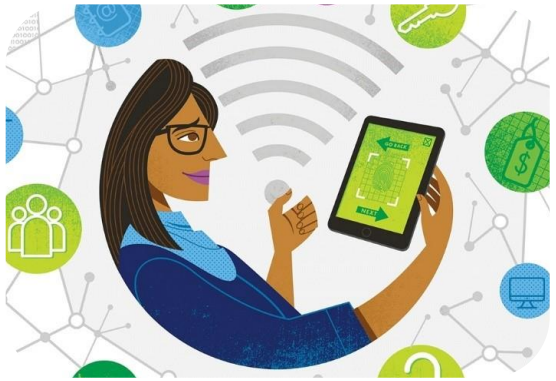
This power point is provided to assist in understanding the draft Data Protection Regulations. It does not form part of the Draft Regulations. The draft Data Protection Regulations which are public documents and are available online are the only authoritative documents

DATA PROTETION (GENERAL) REGULATIONS, 2021

SCOPE OF THE REGULATIONS

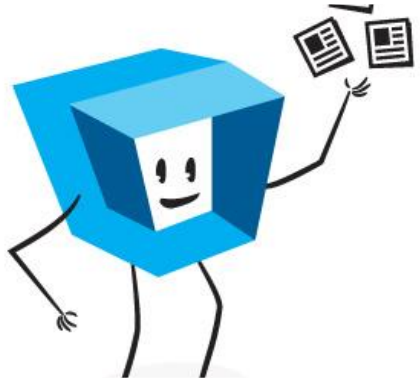
1. Consent of the Data Subject
2. Collection of Personal Data
3. Enabling the rights of the Data Subjects
4. Commercial Use of Personal Data
5. Obligations of Data controllers and Data Processors
6. Data Protection by Design or Default
7. Notification of Personal Data Breaches
8. Transfer of Personal Data Outside Kenya
9. Data Protection Impact Assessment
10. Exemptions.

CONSENT OF THE DATA SUBJECT



Nature of personal data to be processed

Scope of the personal data to be processed



Reasons for processing the required personal data

Whether the personal data shall be shared with third parties.

In obtaining the consent, the data controller and the data processor shall ensure that the:

1. The Data subject has capacity to understand and communicate their consent
2. Data Subject is informed of the nature of processing in simple and clear language that is understandable
3. Data Subject voluntarily gives consent
4. Consent is specific

Consent may be oral, in writing and may include a hand written signature, an oral statement or the use of an electronic or other medium to signify consent.

COLLECTION OF PERSONAL DATA

Collection of personal data entails obtaining personal data directly from the data subject or by any means including from—

- Any other person
- Generally available publications or databases
- Surveillance cameras, where an individual is identifiable or reasonably identifiable
- Information associated with web-browsing, including information collected by cookies
- Biometric technologies.

Data Controllers and Data Processors shall have regard to the following during data collection

- Data Minimisation – collecting what one is permitted to under the law.
- Ensure data quality and accuracy
- Secure the personal data collected
- Only collect sensitive personal data from the data subject

Rights of Data Subjects

- Right to access personal data
- Right to restrict processing
- Right to object to processing
- Right of rectification
- Data portability request
- Right of erasure

Commercial Use of Personal Data

Commercial Purposes	Permitted commercial uses of personal data
Sending a catalogue to a data subject through any medium	No use of sensitive personal for commercial purposes.
Advertisement on an online media site a data subject is logged on using their personal data, including data collected by cookies, relating to a website the data subject has used.	Personal data has been collected from the data subject
Sending an electronic message to a data subject about a sale or other advertisement material relating to a sale using their personal data.	Data subject has been notified of the commercial use, and
	Data subject has consent to the use, and
	The data subject is provided with an opt out mechanism.

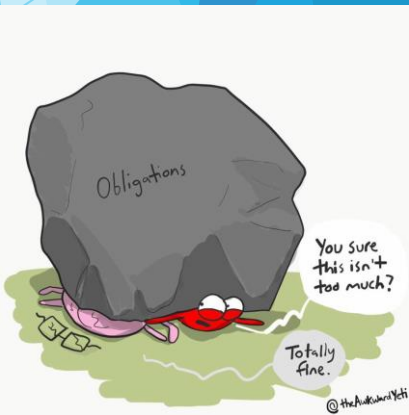
Mechanisms and features to comply with opt out requirements

Features of opting out mechanisms	Visible clear and easy to understand explanation of how to opt out
	Simplified process for opting out requiring minimum time and effort.
	Direct and accessible communication channel.
	Involving nominal cost/ free to the data subject.
	Takes into consideration persons living with disability.

Mechanisms to comply wit opting out requirements	Prominent statement drawing the data subjects to the opt out options.
	Clearly indicate in each direct marketing message that the data subject can opt out of receiving future communications
	Ensure that the opt out procedure is as easy as possible
	Provide the Data Subject with various option of opting out of the direct marketing communications.

Obligations of Data controllers and Data Processors

- Limitation on the retention of personal data
- Requests to anonymize or Pseudonymize personal data
- Sharing of personal data
- Automated individual decision making
- Data protection Policy
- Agreements between data controllers and data processors
- Engagement of a third party in the processing activities.



Data Localization requirements

Data Localization meaning:

a) Processed through a server and data centre located in Kenya,

b) At least one serving copy of the personal data is stored in a data centre located in Kenya.

Purpose – Actualizing a public good:

a) National civil registration systems

b) Population register and identity management

c) Facilitation of primary and secondary education

d) Management of any electronic payment systems

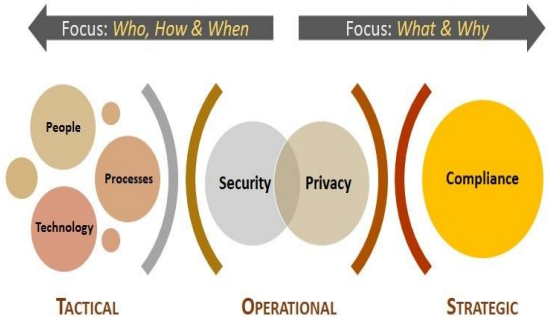
e) Revenue administrations for public finances

f) Processing of health data for any other purpose other than providing healthcare directly to the data subject.

g) Protected computer systems under the Computer Misuse and Cybercrimes Act.

Data Protection by Design or by Default Elements

- Lawful Processing
- Transparency
- Purpose Limitation
- Integrity, confidentiality & availability
- Data Minimization
- Accuracy
- Storage limitation



Notification of Personal Data Breaches

- A data breach is taken to result in real risk of harm to a data subject if that data breach relates to identifiable personal information regarding data subject and includes data such as:
  - (i) the data subject's full name
  - (ii) identification number
  - (iii) account information relating to a data subject
  - (iv) health and treatment information
  - (v) investment and financial information
  - (vi) passwords, security codes etc.

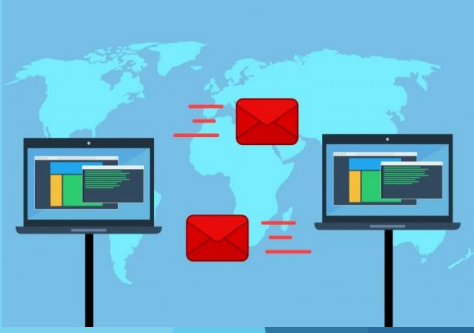
- The personal data or classes of personal data for the purposes of notifiable beaches exclude —
  - (i) any personal data that is publicly available, except if it is public solely because of a data breach; or
  - (ii) any personal data that is disclosed to the extent that is required or permitted under any written law.

Notification of Personal Data Breaches

- A notification of a data breach to the Data Commissioner shall include:

1. Date and circumstances of the personal data breach
2. Chronological account of the steps taken and the assessment of the data breach
3. Details of how the breach occurred
4. Number of the data subjects affected by the data breach
5. Classes of personal data affected by the data breach
6. Potential harm to the affected data subjects
7. Information on any actions taken to eliminate or mitigate any potential harm and to address or remedy any failure or short comings.

Transfer of Personal Data Outside Kenya



- Requirements prior to transfer:

1. Legally enforceable obligations; and
2. Consent to transfer from data subject.

- Cross Boarder transfer Agreements
- Legally enforceable obligations

- Any country or a territory is taken to have appropriate safeguards for purposes of section 49(1) if the country or territory has:

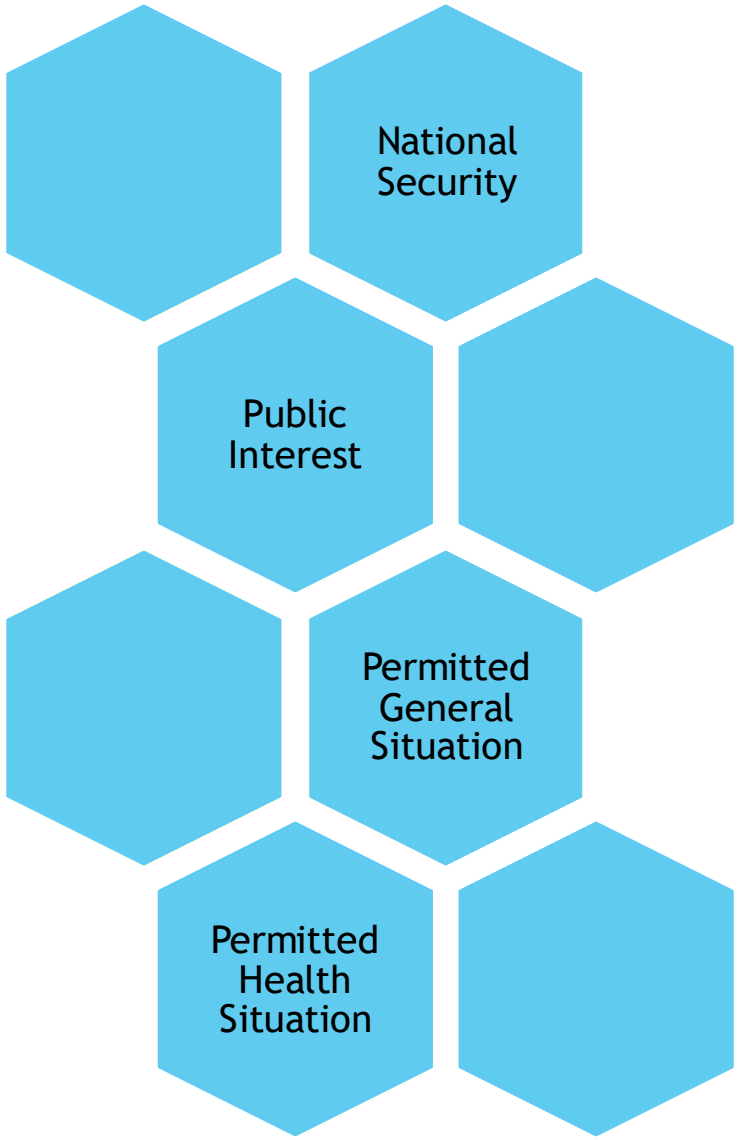
1. Ratified the African Union Convention on Cyber Security and Personal Data Protection;
2. Reciprocal data protection agreement with Kenya
3. An adequate data protection law as shall be determined by the Data Commissioner.

Data Protection Impact Assessment

- High risk activities requiring Data Protection Impact Assessment.

1. automated decision making with legal or similar significant effect.
2. use of personal data on a large-scale for a purpose other than that for which it was initially collected.
3. processing biometric or genetic data
4. a single processing operation or a group of similar processing operations
5. financial and reputational benefits, demonstrating accountability and building trust and engagement with data subjects;
6. where there is a change in any aspect of the processing that may result in higher risk to data subjects
7. processing sensitive personal data or data relating to children or vulnerable groups
8. combining, linking or cross-referencing separate datasets where the data sets are combined from different sources and where processing is carried out for different purposes

Provisions of Exemptions



General Provisions

- Compounding of offences

The Data Commissioner may, with the concurrence of the Office of the Director of Public Prosecutions and with the written consent of the person who commits an offence –

a. Compound an offence under section 58 (8) and section 74 of the Data Protection Act.
b. Make an order for payment by that person of an amount not exceeding 2/3 of the maximum penalty that would have been imposed on conviction.

On Compounding of the offence the Data Commissioner shall:

Make an order in writing and attach the admission of the offered and the occurrence of the ODPP

Specify the offence committed and the amount to be paid and the date of the payment

Give the offender a copy of the order upon request.

PLENARY SESSION
Q&A

Comments and concerns can be sent to the following email address;

dataprotectionregulations@odpc.go.ke

The End