Data Protection in a Fintech context

What does Good look like?

1

Agenda

Context setting

Background to the documents published and the resources available

Establishing a Team

Where is the data?

Finding the hidden data

Implementing a Data Protection Impact Assessment

Tools and Resources to get started

Agenda

Context setting

Background to the documents published and the resources available

Establishing a Team

Where is the data?

Finding the hidden data

Implementing a Data Protection Impact Assessment

Tools and Resources to get started

Access to Data creates Opportunity for Better: – regulators globally are leading this conversation

3 resources:

- https://www.cgap.org/sites/default/files/event_documents/Open_Banking_Webinar_Presentation_Oct142020.pdf
- https://www.cgap.org/research/publication/open-banking-how-design-financial-inclusion
- https://www.cgap.org/blog/open-banking-7-ways-data-sharing-can-advance-financial-inclusion

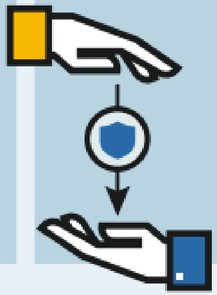
fsd Kenya

Global Regulatory trends point to putting the responsibility on the service provider in law

https://www.cgap.org/sites/default/files/publications/2020_01_Focus_Note_Making_Data_Work_for_Poor_0.pdf

CGAP's Three Recommendations

1



Shift Onus Onto Provider
Place new responsibilities onto data collectors and processors, rather than relying on consumer consent. Two options:

Legitimate Purposes Test
Only allowed to use data in ways that benefit the customer;

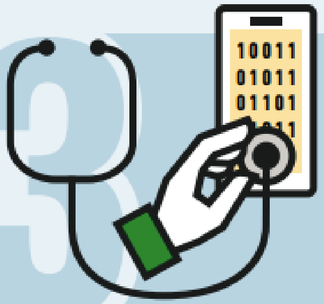
OR

2

Digital Bill of Rights
Empower consumers to control their own data by allowing them to easily access, correct and port data free of charge.

Fiduciary Duty
Must always act in the interests of the customer.

3



Privacy Representatives
Ensure fairness in processing of data through privacy representatives who can review consumers' data profiles and check algorithmic models for fairness, bias and exclusion.

European GDPR law is creating consequences for those who breach it.

Record €225m fine for WhatsApp Ireland over data protection breaches

Updated / Thursday, 2 Sep 2021 14:31

WhatsApp Ireland's fine is the second largest penalty ever levied on an organisation under EU data laws

But Is Data Privacy about Compliance or Good Business? CGAP found that poor customers:

- Prefer privacy, if they have a choice, and are willing to pay for it.
- Will invest time in obtaining a loan that offers privacy.
- Are least willing to share data with third parties.

Offering products that have strong data privacy and protections built in could give an edge in a competitive marketplace.

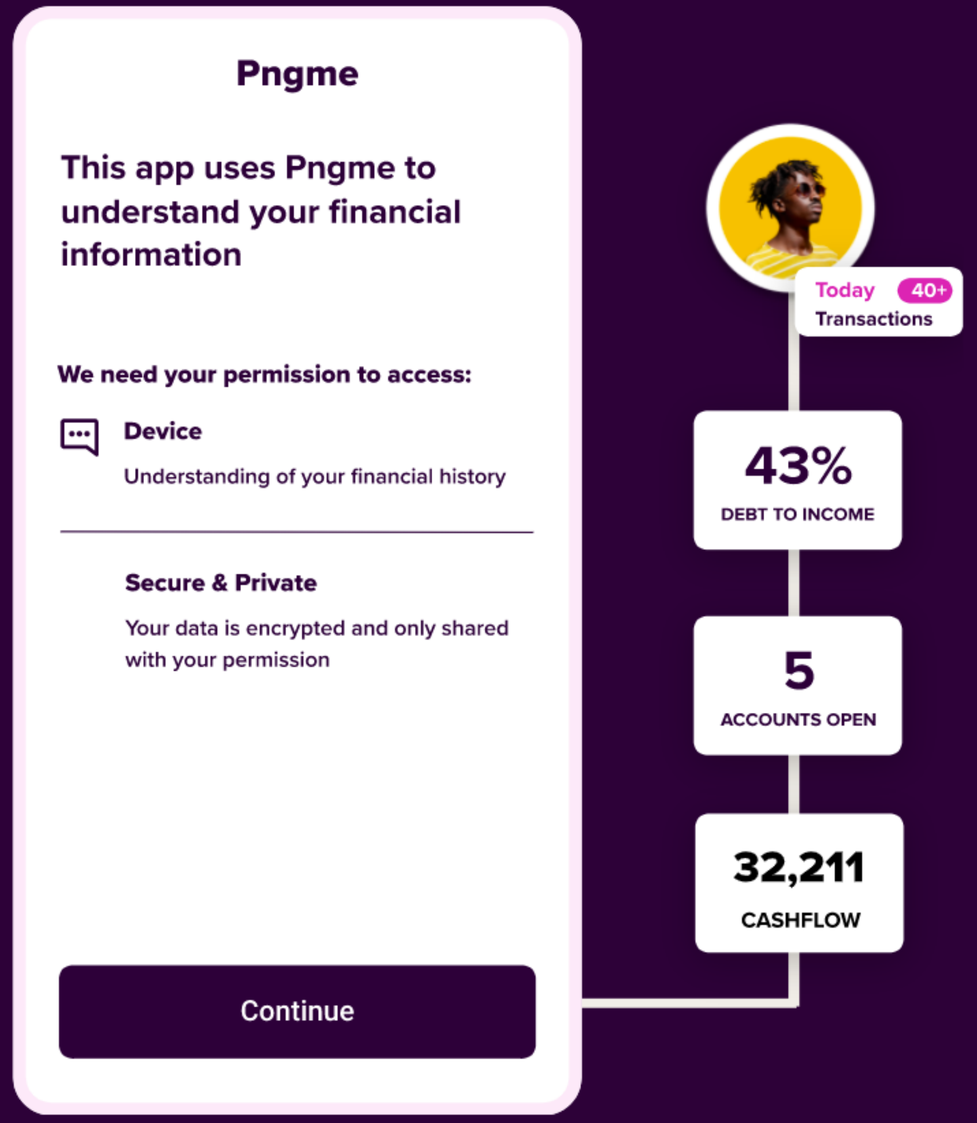
https://www.cgap.org/sites/default/files/publications/2019_12_Focus_Note_Is_Data_Privacy_Good_for_Business_1.pdf

The leading financial data platform

Mission critical data infrastructure and machine learning models powering the next generation of financial services

Talk to us

Learn more



Africa's Talking CredPal INLAKS PAVELON readycash SimpleFi

HOW IT WORKS

Tackling data challenges

We provide three key services to overcome these challenges

Seamless project setup

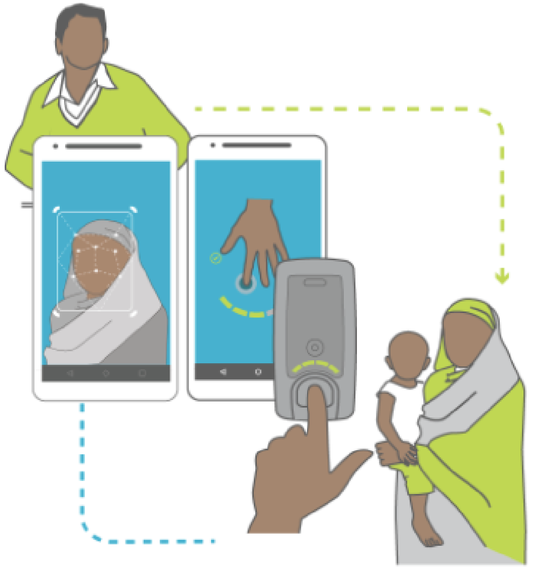
Robust identification tools

Data analytics and support

PORTABLE, PRACTICAL, PEOPLE-CENTRED

Robust identification tools

Using a wireless biometric scanner, a mobile app, and the cloud, Simprints enrols and matches people to their digital records with a touch of a finger.



Disclaimer

This document is neither intended to provide legal advice nor should it be relied upon as a source of legal advice. The information is meant to be general and educational in nature and the materials and references provided in the document may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on one’s circumstances.

Agenda

Context setting

Background to the documents published and the resources available

Establishing a Team

Where is the data?

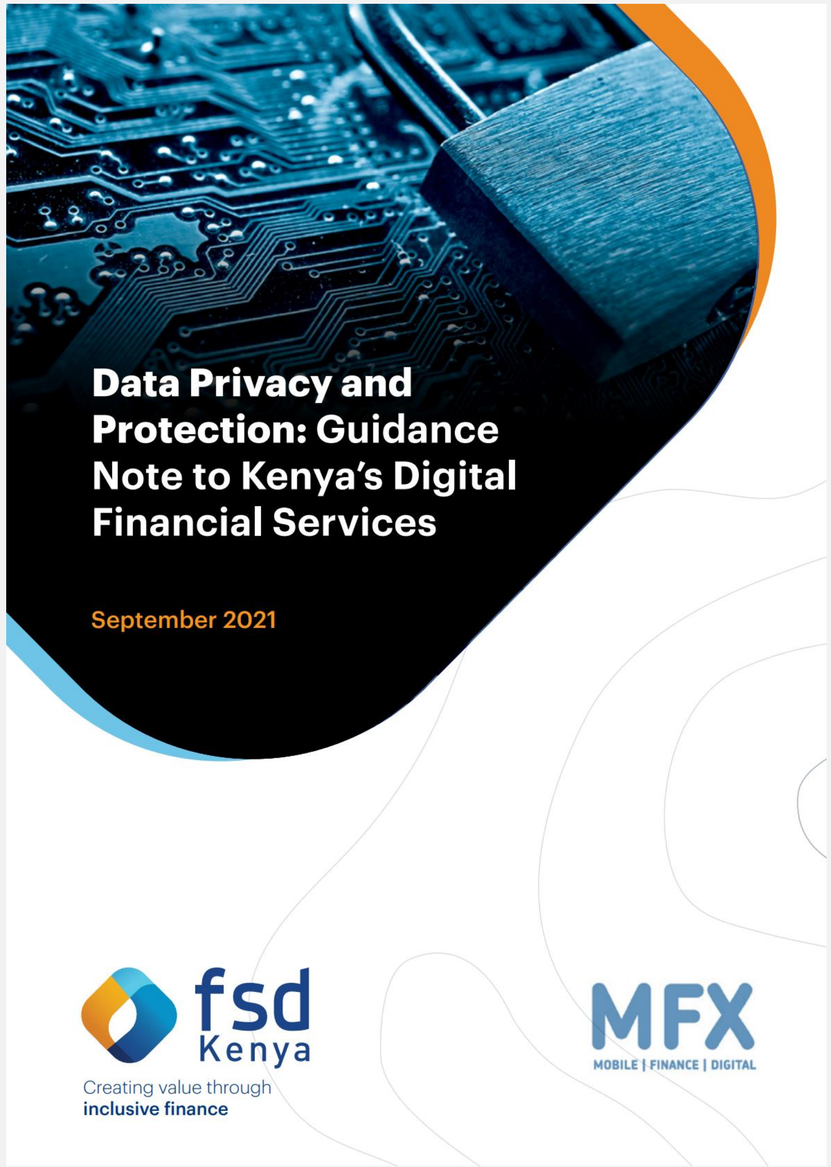
Finding the hidden data

Implementing a Data Protection Impact Assessment

Tools and Resources to get started

Background to the documents published and the resources available

The target audience for each document and where to get them
How to keep abreast of changes in regulation in Kenya and globally?
Case study on regulatory review: customer consent
Examples of consent done well, and consent not done well



3 documents made available

- Implementation Guidance
  https://www.fsdkenya.org/wp-content/uploads/2021/08/DAPA-Report-08272021.pdf

- Regulatory review
  Issued soon

- Policy Recommendation
  Issued soon

The primary focus for all the documents has been the Financial Services domain, but other industries may find some benefits

fsd Kenya

Data Privacy and Protection: Guidance Note to Kenya's Digital Financial Services

September 2021

fsd Kenya

Creating value through **inclusive finance**

MFX

MOBILE | FINANCE | DIGITAL

Implementation Guidance

Aimed at Product Managers and IT Managers working in Fintech's in Kenya trying to identify the next steps of their implementation of the Kenyan Data Protection Act (DAPA).

fsd Kenya

Key Sections

- Fintech Understanding of the Data Protection Act in Kenya
  - Assessing the knowledge and awareness of those responding on the existing legislation, as well as their existing implementation
- Data Protection in a Fintech Context
- Implementation Examples

We should be driven by Data – so…

Who responded?

We had a small, but representative response

Figure 1: Size of Company (No. of employees)

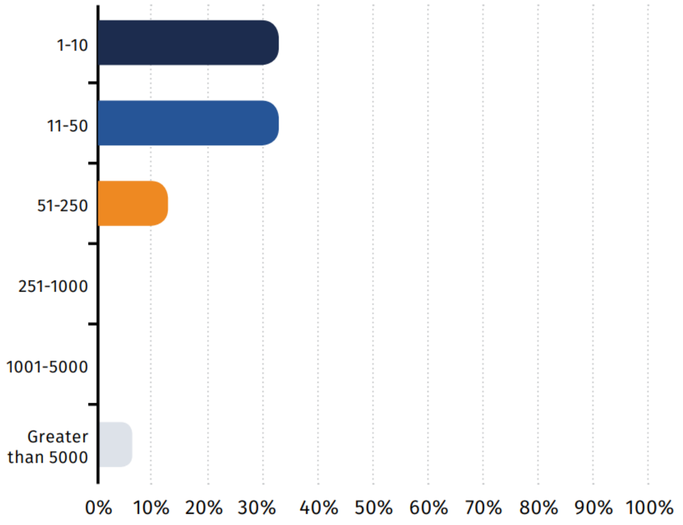
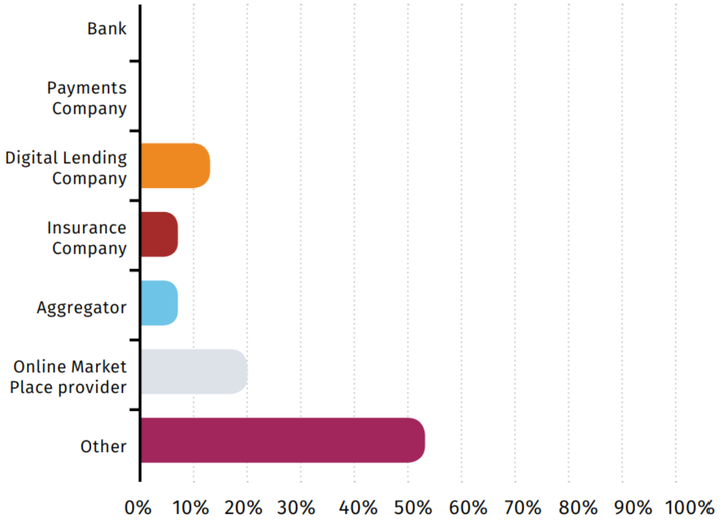
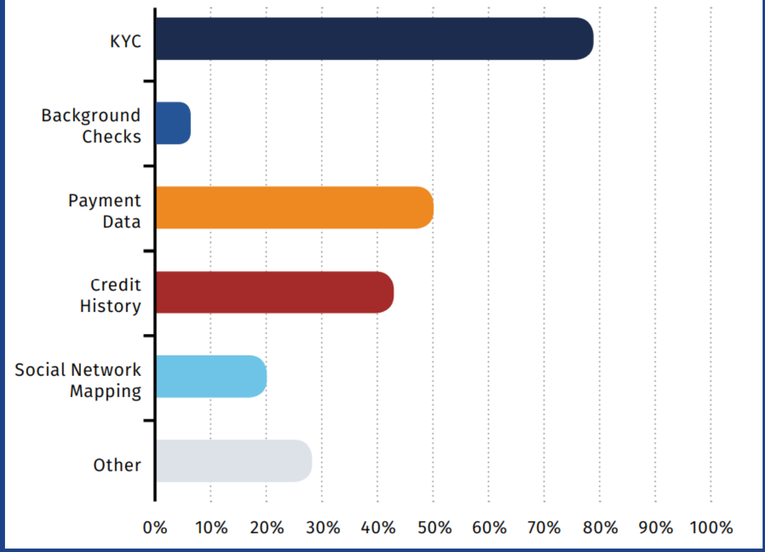


Figure 2: Types of Company



With KYC Data being most used

Figure 3: Types of personal data processed



What are they currently doing?

None of the respondents had appointed a dedicated DPO

Not many were appointing a senior person

Figure 6: For those yet to recruit, is there a plan to recruit for the role?

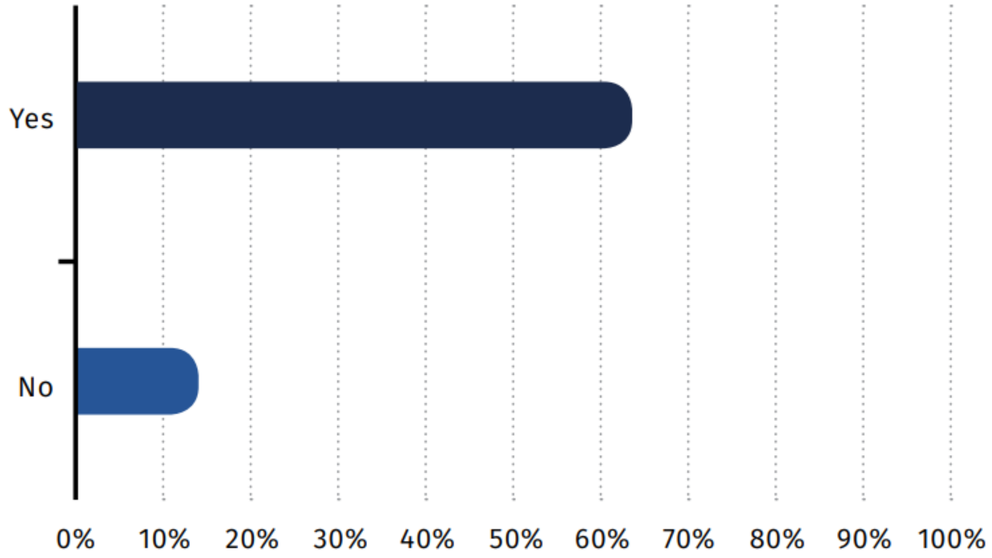
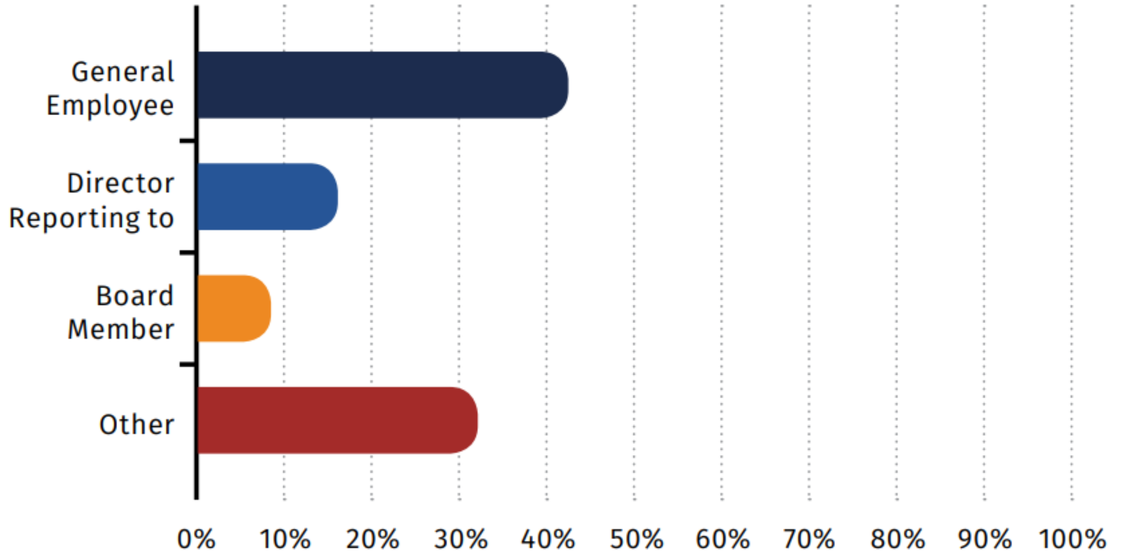


Figure 7: For all – what is the expected seniority of this role or person taking responsibility for the task?



Do they share, and how did they get customer permission?

Nearly all the responding parties also shared their data with other parties. For over 60% of respondents, the data subjects had been asked permission for this sharing in their contracts

Figure 8: Do you share data with other parties?

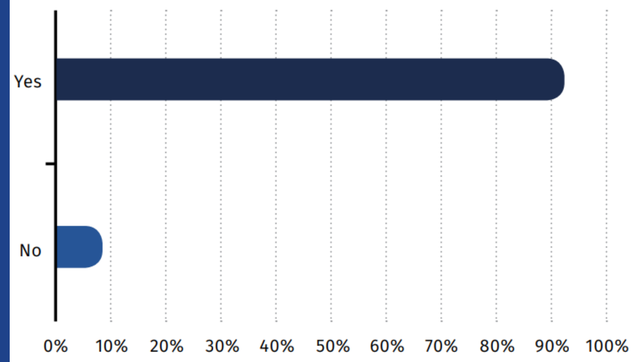
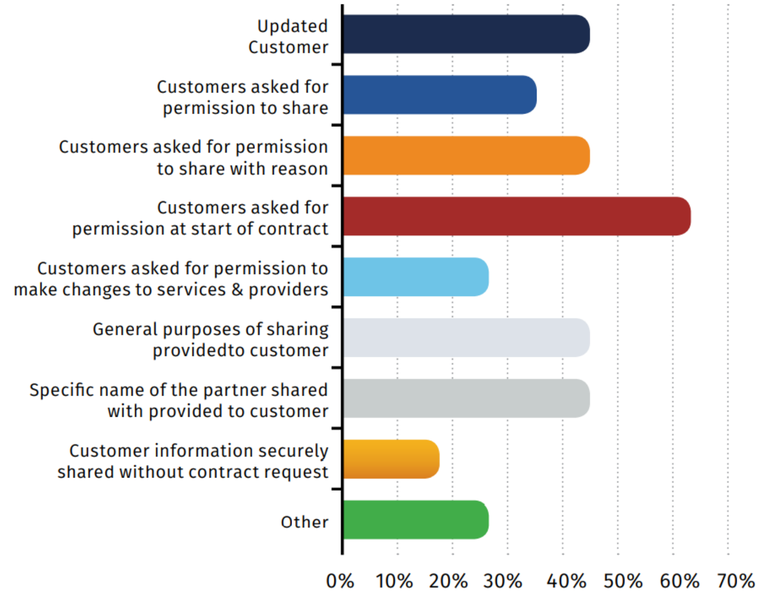


Figure 9: What controls do you already have in place?



Have they started to make changes?

Only 33% of respondents had a specific and dedicated project, but some had started improvements whilst the act was still a bill

Figure 10: Have you implemented a programme to deliver the requirements of the Act?

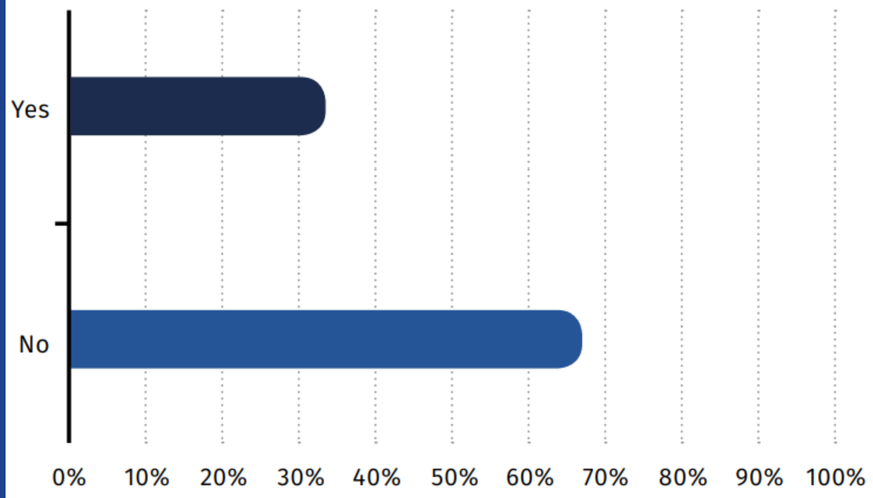
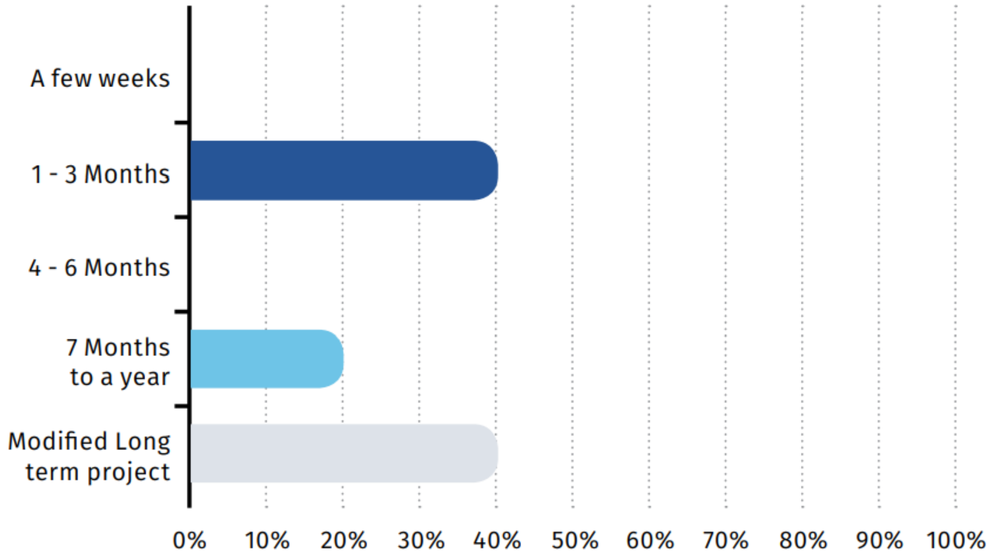


Figure 11: If yes - how long has it been running?



How was the act perceived?

Opportunities

- Enhance the level of trust in fintechs.
- A means of weeding out bad practices, and as an honor badge for compliant fintechs.
- An increased uptake of solutions provided by fintechs.
- The responsibility to protect sensitive data as an opportunity to enhance their contracts with data processors, now that there is better clarity on where responsibility lies.
- improve their business processes and structure their data to eliminate ‘noise’ in their current processes.
- Some respondents also see opportunities for their data subjects with regards to opportunities to leverage their data for better solutions and services, especially through data portability.

Challenges

- A lack of guidance, and the risk that individual interpretations can lead to inconsistent application of the law.
  - Smaller firms felt that their processes were disproportionately constrained by the lack of guidance on implementation.
- The of unique challenges that are pertinent to Kenya, for example managing consent on channels such as USSD.
- The risk of unscrupulous data subjects who start baseless disputes to seek financial compensation.

Data Privacy and Protection: Guidance Note to Kenya's Digital Financial Services

September 2021

The remaining chapters of the document will be addressed in the webinar

A Review Of The Regulatory Framework For Data Protection In Kenya

fsd Kenya
Creating value through inclusive finance

MFX
MOBILE | FINANCE | DIGITAL

Regulatory Framework

Aimed at Data Protection Officers and Regulatory advisors it provides an overview of the act and what it might mean to those implementing it

It assesses the strengths and weaknesses of the Act and Regulation as well as suggestions on potential improvements – when compared to the approach of other regulators around the world

For those working with international customers, it also provides guidance on GDPR and CCPA

fsd Kenya

Key Sections

- Understanding the Data Protection Act
  - Lawfulness / Fairness / Transparency
  - Purpose Limitation
  - Data Minimisation
  - Accuracy
  - Storage Limitation
  - Integrity & Confidentiality / Security
  - Accountability
- Guidance Provided by other Regulators

Why Compare DAPA with CCPA and GDPR?

- All global companies have already implemented the necessary changes to comply with both GDPR and CCPA.
- The prominence of Technology companies and Venture Capital companies based in California, with CCPA being introduced heightened the awareness of the need for tech companies to address the protection of consumers' data.
- GDPR provides the most comprehensive data protection laws in the world to date. There is a large volume of work that can be used to support any government looking to implement a data protection strategy for her citizens
- CCPA is a first of its kind for the USA, and currently there are no other plans for a federal privacy law in the U.S. Given the State of California alone is equivalent to the fifth largest global economy, its effectiveness will be a key point of impact and interest for the remainder of the world.

How to carve up the legislation?

- As most regulation has been based on the same foundational principles – we used those principles to identify key questions driven from the survey.

- For each question we provided
  - a summary and guidance on the implications of the legislation
  - Policy Recommendations where appropriate
  - Collated the relevant legislation for improved reference

- Foundation Principles
  - Lawfulness / Fairness / Transparency
  - Purpose Limitation
  - Data Minimisation
  - Accuracy
  - Storage Limitation
  - Integrity & Confidentiality / Security
  - Accountability

Guidance Provided by other Regulators

- We explore the approach taken by other regulators to inform Citizens as well as the Data Controllers and Processors
- UK
  - A large volume of insight is available from the Information Commissioner's Office (ICO)
  - There are insights and guidance for Consumers and Organisations
  - There are also self assessments that allow an organisation to know the steps they need to perform
- Netherlands
  - The Netherlands "English site" ensures the impact of failing to comply are always front of mind
  - The Dutch site provides a more detailed approach – similar to that of the UK
- South Africa
  - Provides a site that is betters suited to lawyers
- Singapore
  - Provides clear guidance, and allows for a more detailed drill down where required

But the passing of the Act is just the start

1. The Office of the Data Protection Commissioner (ODPC) is regularly updating their website: https://www.odpc.go.ke
2. With General guidelines being made available in https://www.odpc.go.ke/documents/

In addition to highlighting the work underway to establish the Kenya Data Protection Act, The ODPC is clearly putting consumers first

Key Sections

1. *Take Action*
2. *Data Subjects*
3. *Data Controllers and Processors*
4. *Resources*

fsd Kenya

Guidance on Consent

- Covered specifically in Section 30 of the act
- Further guidance provided on Consent to take account of:
  - The Act
  - The Privacy and Data Protection Policy
  - International Best Practice

Legal Basis for Processing of Data

The act provides eight legal grounds:

1. the data subject consents to the processing for one or more specified purposes; or the processing is necessary
2. for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract
3. for compliance with any legal obligation to which the controller is subject;
4. to protect the vital interests of the data subject or another natural person;
5. for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
6. the performance of any task carried out by a public authority
7. for the exercise, by any person in the public interest, of any other functions of a public nature;
8. for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or (viii) for the purpose of historical, statistical, journalistic, literature and art or scientific research.

Guidelines were issued to clarify Consent

Appropriate Lawful Basis IF the data subject is offered:

- Control
- A genuine choice about accepting or declining the terms
- Declining them without detriment

Data controllers and Data subjects run the risk consent will be ignored if it is **illusory**

The balance of Section 25 of the Act in relation to fairness, necessity and proportionality require controllers to **ask some Key Questions** - consent alone is not the only measure

- **Is this necessary for the specified purposes**
- **Is it fundamentally unfair**

The application of the terms “FREE” and “INFORMED” brings a much stronger onus – with Clarity and Simplicity being the focus

What does a Controller have to provide:

- The data controller and data processor's identity – as well as those of third parties relying on the consent
- The purposes of the processing: It must cover all purposes
- The processing activities: Granular consent for each separate type of processing
- The right to withdraw consent: including how to exercise that right

Consent needs to be a "Clear Affirmative Act"

Lawful basis needs to be applied consistently

I captured customer data before the act?

- Consent obtained before the act will remain valid
- The consent must be in line with the act and validly obtained
- This will also need to be reviewed as the purposes change
- Those processing data that is “likely to result in a high risk” to data subjects should submit a DPIA

Some examples of good and bad consent

- We have already seen how the Information Commissioners use Cookies to capture consent
- Bluewave (bluewaveinsurance.co)
- There are then bad examples – invariably where advertising is their key revenue e.g. online newspapers or merchant stores

Agenda

Context setting

Background to the documents published and the resources available

Establishing a Team

Where is the data?

Finding the hidden data

Implementing a Data Protection Impact Assessment

Tools and Resources to get started

Establishing a Team

- Beyond the legislation – what are the key drivers to implementing a data protection programme?
- Does an organization need a Data Protection Officer? If so, what is the seniority and profile of the role?
- What other resources might an organization need?
- What are some of the operational impacts to consider?

Key Drivers to implementing a programme

- The fines alone will not encourage strong company investment
- Reputational impact can be a driver, but this will only be relevant if failures are highlighted by the ODPC

- Companies who focus on providing a great user experience, and protection of their customers can use the legislation as an opportunity to highlight how they are transparent and protect their customers

Do I need a Data Protection Officer?

- A data controller or data processor may designate or appoint a data protection officer. A data protection officer may be a staff member of the data controller or data processor and may fulfil other tasks and duties provided that any such tasks and duties do not result in a conflict of interest.
- A person may be designated or appointed as a data protection officer, if that person has relevant academic or professional qualifications which may include knowledge and technical skills in matters relating to data protection

What else should they focus on

- A data controller or data processor shall publish the contact details of the data protection officer on the website and communicate them to the Data Commissioner who shall ensure that the same information is available on the official website.

- A data protection officer shall: advise the data controller or data processor and their employees on data processing requirements provided under this Act or any other written law; ensure on behalf of the data controller or data processor that this Act is complied with; facilitate capacity building of staff involved in data processing operations; provide advice on data protection impact assessment

I have a DPO – is that it?

- The DPO has to ensure that all staff are aware of the act, and what they need to do differently
- The larger your organisation, the more people that will need to input to the DPO – so you actually understand all the data you are processing
  - You will need input from all areas of the business where customer or Employee data is captured or processed
  - Sales, Marketing, Customer Support, Finance, HR, IT etc.
  - The use of area champions will be critical

Assessment team in place – JOB DONE

- Unfortunately this is just the start of the journey
- The impact of DAPA will require:
  - Clarity on the Purposes you have
  - New terms and conditions
  - Implementation of any new controls or processes
  - Change in flows to collect consent and store this for as long as needed (consider any agent based work)
  - Remove any data where consent is not clear
  - Manage changes in consent
  - Restrict processes when consent is changed
  - Managing Data Subject Access Requests
  - Managing Data Change Requests
  - Managing Data Porting Requests
  - Managing Data Breaches

So – What is a Data Process Impact Assessment (DPIA)

- Before processing a consumers data, a Data controller or processor should submit a DPIA to the office of the data commissioner
- ODPC has issued further guidance since the act was made law
  - *"A DPIA describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and early as possible"*
- The controls can be technical or organisational
- Data Protection should be by design and/or default
- The DPIA needs to be submitted to the ODPC

What does a DPIA need to include

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller or data processor
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes
- An assessment of the risks to the rights and freedoms of data subjects
- It is NOT mandatory – but it is a pre-requisite when the processing of personal data is "likely to result in a high risk to the rights and freedoms of data subjects".

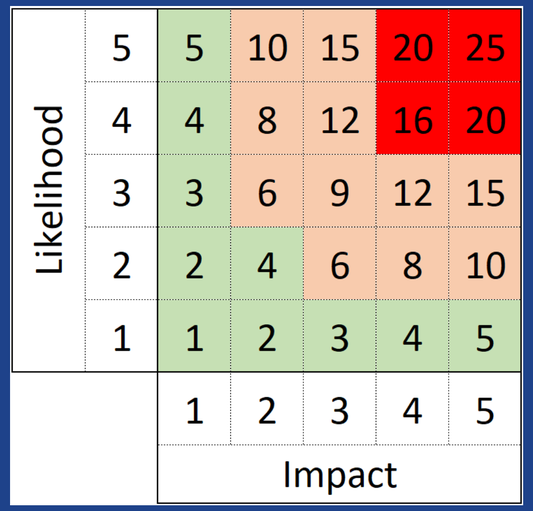
What areas does a DPIA need to cover

- Automated decision making with legal or similar significant effect
- Systematic Monitoring
- Sensitive personal data
- Data processed on a large volume or large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects
- Innovative user or applying new technological or organisational solutions
- When the processing in itself prevents data subjects from exercising a right

A quick tour of a risk assessment

- On pages 12-17 of the ODPC guidance, they have provided a DPIA for, on Page 16 they provide a Risk Register
- For those who have not used a risk register before – there are some fields missing on this form
- The ODPC is interested in Residual Risk
- A risk manager is interested in:
  - the inherent risk (risk before controls are considered)
  - Effectiveness of controls
  - Residual risk (exposure after controls are considered)

Getting our heads around things



- There are two variables that we are working with when assessing a risk
  - Likelihood (how likely is it something will go wrong)
  - Impact (if things go wrong is it
  - Both use a scale of 1-5 (sometimes we state VL, L, M, H, VH)
- Once we determine the Likelihood and Impact of a risk we multiply them together to get an inherent risk score
- We then apply a control – such as encryption
- Then re-assess the score
- Once we have captured all the residual risks, we create a risk heat map to prioritise our activity

Agenda

Context setting

Background to the documents published and the resources available

Establishing a Team

Where is the data?

Finding the hidden data

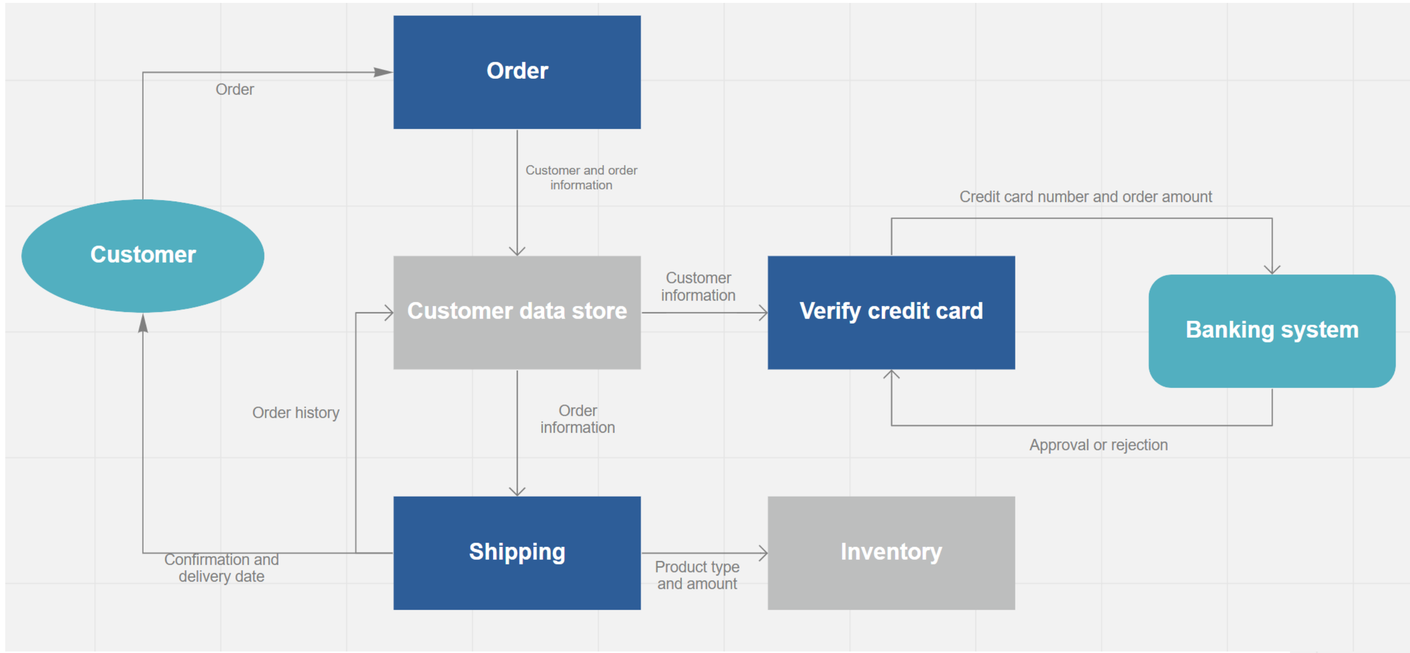
Implementing a Data Protection Impact Assessment

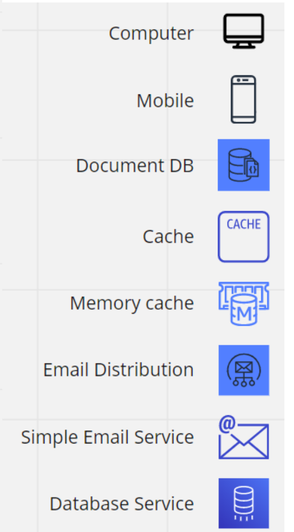
Tools and Resources to get started

Where is the data?

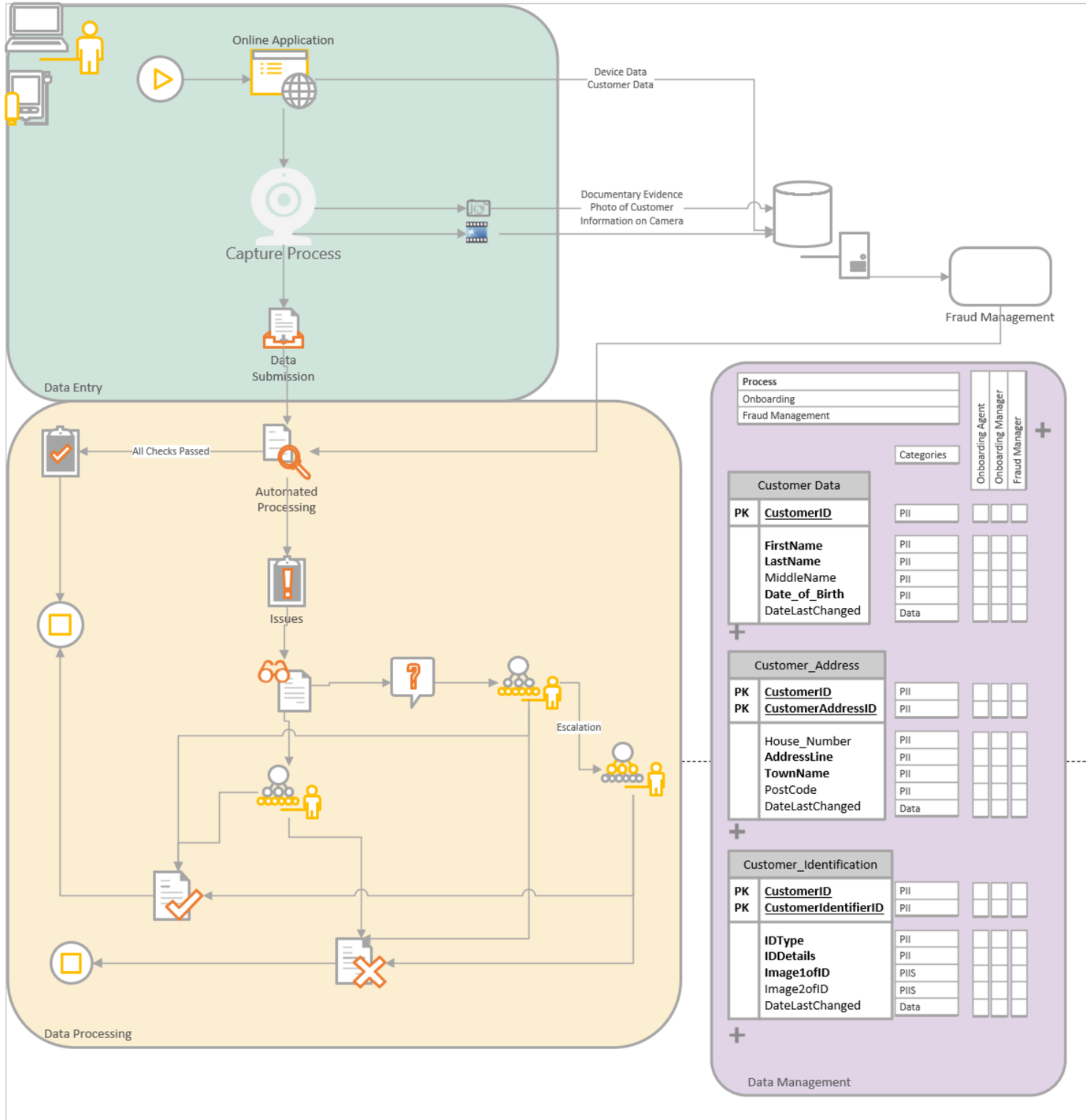
- Identifying all the data creation and collection points
- How to develop a simple process to map showing sources of data, where to store it and how you protect it

Miro Interactive White Board





Visio Process Map



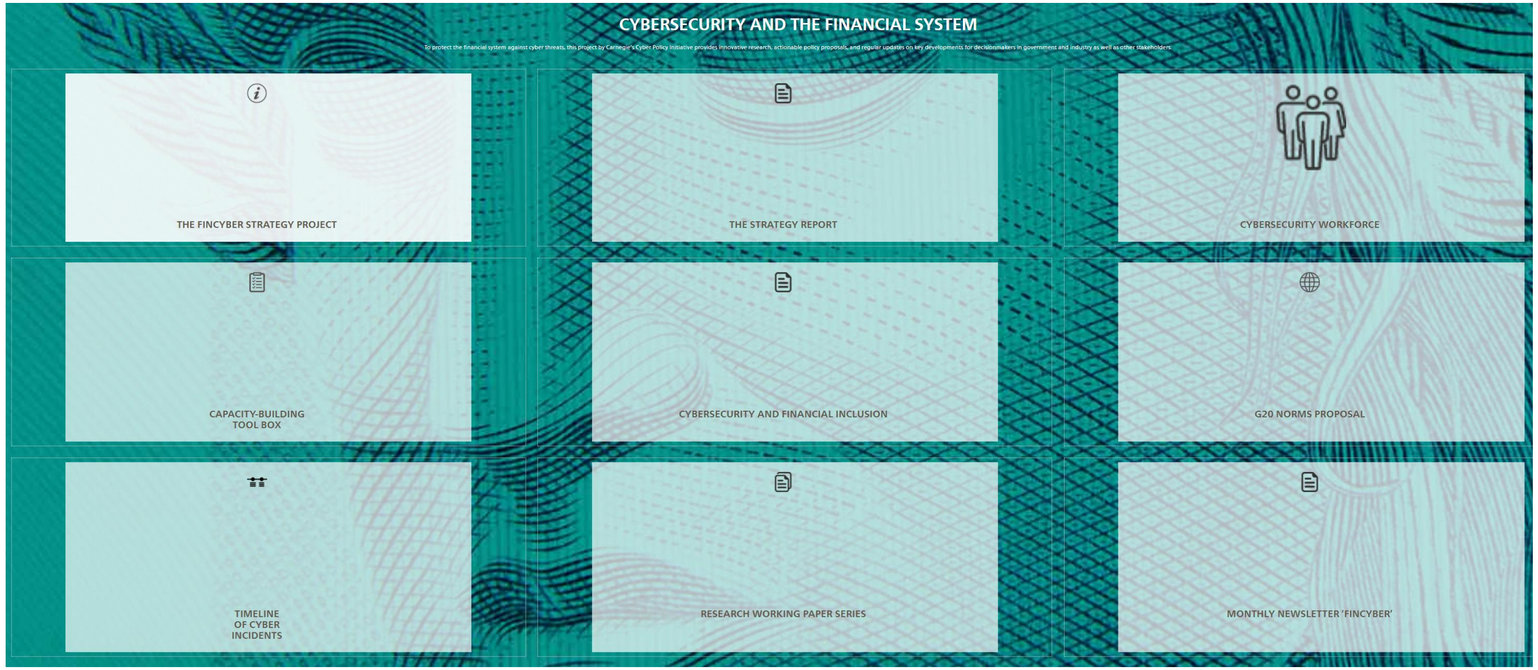
Changes to hosting

- Draft Data Protection General regulations
  - 25.(1) Pursuant to section 50 of the Act, a data controller or data processor who processes personal data for the purpose of actualising a public good set out under paragraph (2) shall be required to ensure that
    - (a) such processing is effected through a server and data centre located in Kenya; and
    - (b) at least one serving copy of the concerned personal data is stored in a data centre located in Kenya.
  - (2) The purpose contemplated under paragraph (1) that require processing in Kenya includes -
    - (a) administering a national civil registration system including registrations of births and deaths, persons, adoption and marriages;
    - (b) operating a population register and identity management system including any issuance of any public document of identity;
    - (c) managing personal data to facilitate access of primary and secondary education in the country;
    - (d) the conduct of elections in the country;
    - (e) managing any electronic payments systems licensed under the National Payment Systems Act;
    - (f) any revenue administration system for public finances;
    - (g) processing health data for any other purpose other than providing health care directly to a data subject; or
    - (h) managing any system designated as a protected computer system in terms of section 20 of the Computer Misuse and Cybercrime Act, 2018.

Unfortunately you also need to consider how you share

- GDPR has led to a growth of Privacy Enhancing Tools (PETs)
- These were explored in the FCA Sandbox Pilot at the beginning of this year
- Digital Sandbox (digitalsandboxpilot.co.uk)

Getting Cyber-security help



THE LINUX FOUNDATION PROJECTS

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Agenda

Context setting

Background to the documents published and the resources available

Establishing a Team

Where is the data?

Finding the hidden data

Implementing a Data Protection Impact Assessment

Tools and Resources to get started

Finding the hidden data

- Understanding unstructured data
- Mechanisms to manage the data

What is Unstructured Data?

- Unstructured data is data that is not organised in a predefined manner and is found in images, audio files, presentations, communication channels (such as slack), social media accounts, emails, and documents (including PDFs etc.). This set of data is likely to grow exponentially and therefore become much harder to map: it could equate to 80-90% of a company's data. Finding an owner for unstructured data can be one of the most complex tasks in the inventory process

Some ways of getting to Unstructured Data

- What can your NAS do already
  - Search
  - Intelligent OCR
  - PDF Data extraction
- Suppliers who offer a service

Agenda

Context setting

Background to the documents published and the resources available

Establishing a Team

Where is the data?

Finding the hidden data

Implementing a Data Protection Impact Assessment

Tools and Resources to get started

Implementing a Data Protection Impact Assessment

- What are you obliged to do?
- How to ensure that you focus on the key tasks

What does a DPIA need to include

- A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller or data processor
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes
- An assessment of the risks to the rights and freedoms of data subjects
- It is NOT mandatory – but it is a pre-requisite when the processing of personal data is "likely to result in a high risk to the rights and freedoms of data subjects".

Agenda

Context setting

Background to the documents published and the resources available

Establishing a Team

Where is the data?

Finding the hidden data

Implementing a Data Protection Impact Assessment

Tools and Resources to get started

Tools and Resources to get started

Table of Contents