ADOPTING DPIA IN AFRICA: LESSONS FROM KENYA'S DPIA FRAMEWORK AND EXPERIENCES

Conference: African Data Protection Laws: Regulations, Practice, and Policy

13-15 September 2022

DR IHEANYI SAMUEL NWANKWO & MR NELSON OTIENO OKEYO

Outline

- Background
- DPIA in African Regional, Sub-regional and National Instruments
- DPIA Framework: The Kenyan Example
- Concluding Remarks: Lessons for Africa

BACKGROUND

Common approaches to data protection compliance: EU example

- **Principle-based approach:**

✓ Requirement to comply with data protection principles (E.g., Art. 5 GDPR)

- **Precautionary approach**:

✓ Notification (Art 18 DPD)

✓ Prior checking (Art. 20 DPD, Art. 36 GDPR)

- **Risk-based approach (RBA):**

✓ Mapping obligations in relation to risk possed by the data processing (eg, Arts. 24, 25 and 32 of the GDPR in general, and Art 35 for high-risk processing)

What does the RBA in data protection entail?

- ❑A proactive approach to compliance (ex-ante requirement)
- ❑Using the degree of risk to apportion responsibilities/safeguards
- ❑Measures and strategies to protect personal data must be based on risk analysis (particularly as they affect the rights and freedoms of data subjects)
- ❑Adoption of objective/conventional method of risk management (e.g., ISO 29134, ISO 31000)
- ❑Expansive in nature: it aims at assessing the impact and likelihood of harm to data subjects at both the individual and societal levels

Impact assessment: A tool for implementing the RBA

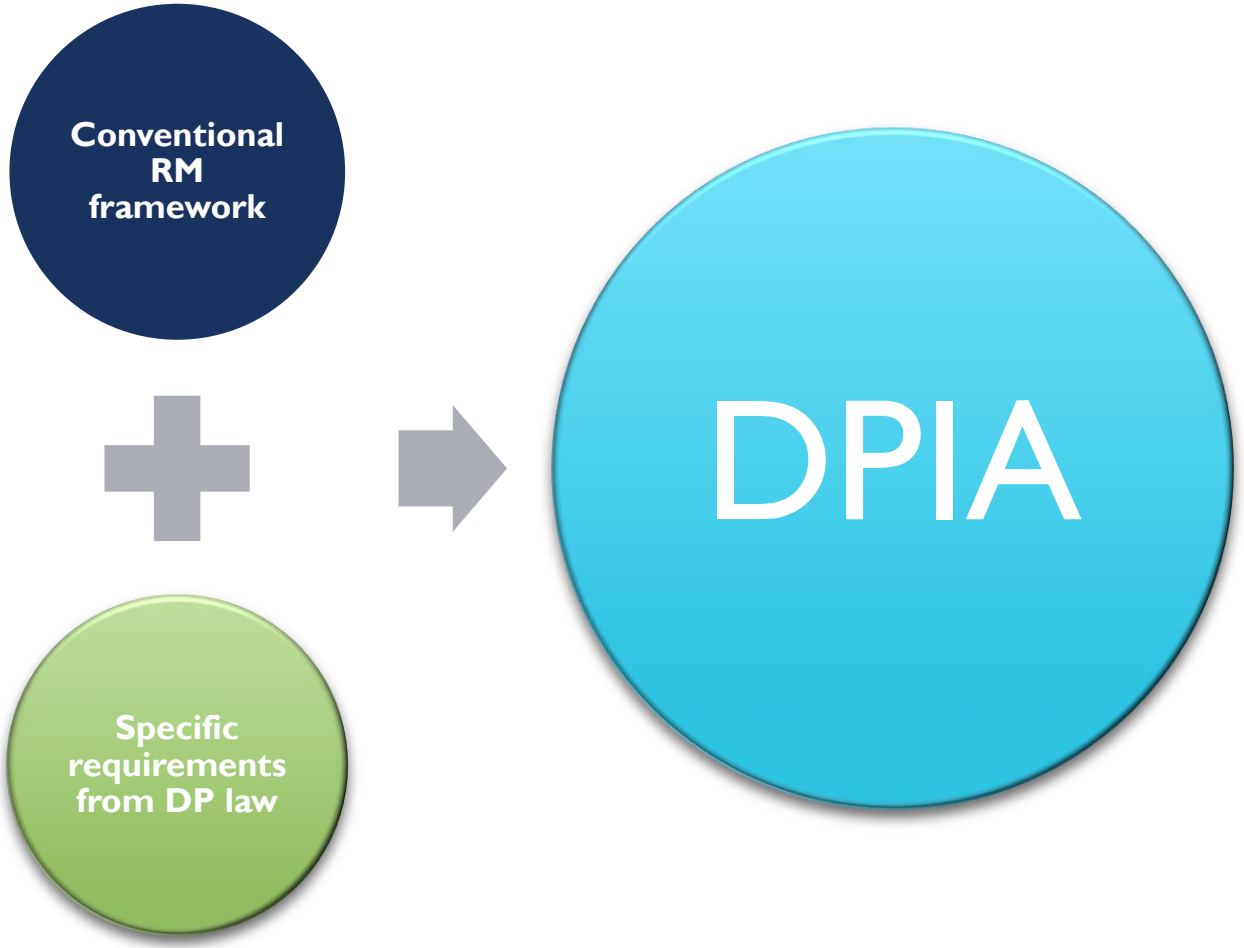
Impact Assessment

A formal, evidence-based prospective analysis to estimate the attributable impact of a project and to inform decision makers accordingly

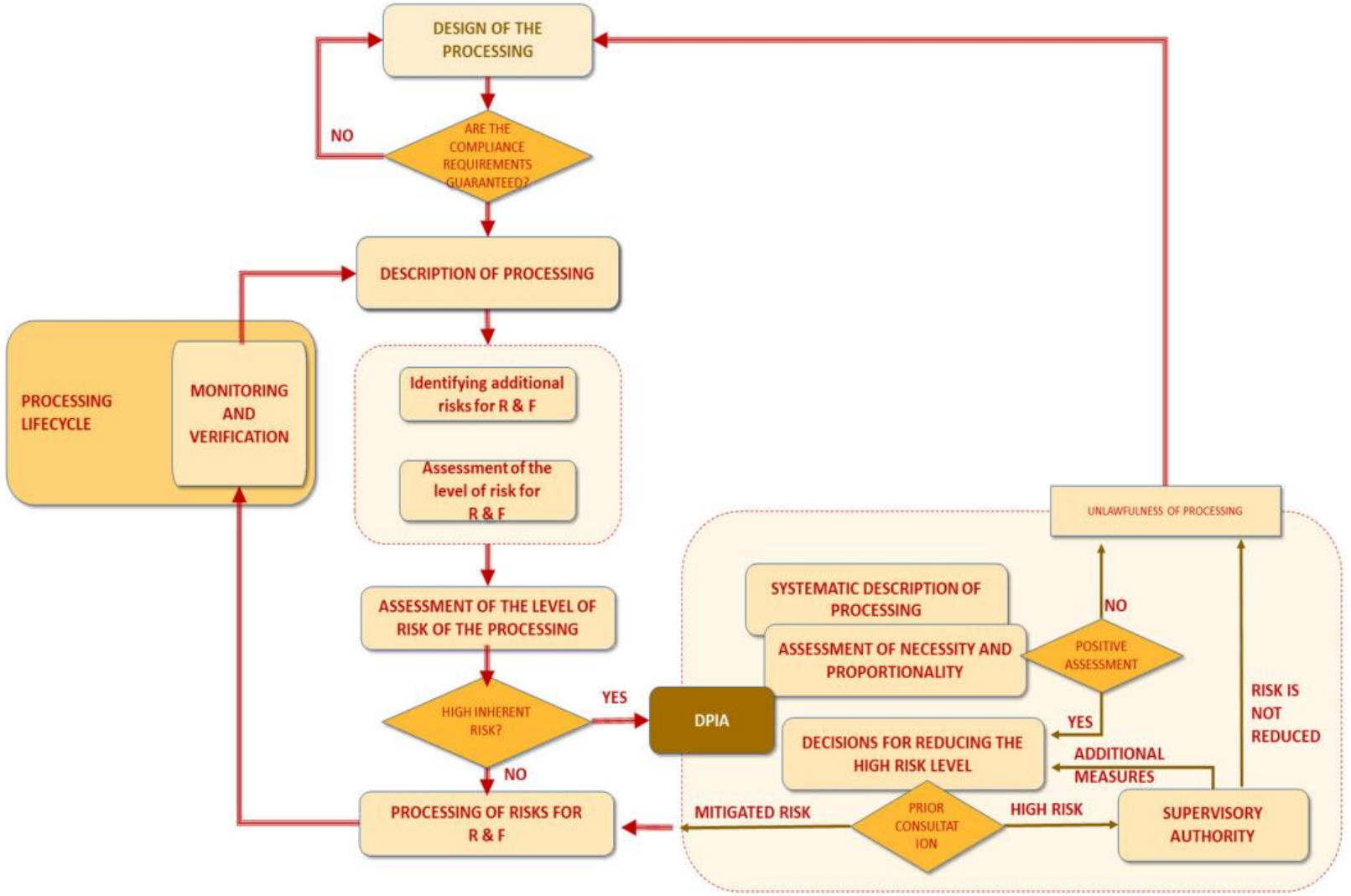
Impact assessment in data protection law

What does impact assessment entail in data protection law?

Systematically identifying and recording the risks associated with a particular data processing operation, which should inform the design of the system and the measures to be adopted to prevent or mitigate these risks



AEPD framework of DPIA within the risk management process



Real world impact: A few examples

The Dutch Microsoft Office 365 DPIA

PRIVACY COMPANY

Home Services Products Factsheets Ab

Impact assessment shows privacy risks in Microsoft Office ProPlus Enterprise

On behalf of the Dutch Ministry of Security and Justice, Privacy Company carried out a (DPIA) on Microsoft Office ProPlus (Office 2016 MSI and Office 365 CTR). With the permission of the Ministry, we publish this blog about our findings. For questions about the research you can contact SLM Rijk (Strategic Vendor Management for Microsoft within the Ministry of Justice), accessible via the Press Office from the Ministry of Justice, +31 (0)70 370 73 45.

The SLM Rijk conducts negotiations with Microsoft for approximately 300,000 digital work stations of the national government. The Enterprise version of the Office software is deployed by different governmental organisations, such as ministries, the judiciary, the police and the taxing authority.

The results of this Data Protection Impact Assessment (DPIA) are alarming. Microsoft collects and stores personal data about the behaviour of individual employees on a large scale, without any public documentation. The DPIA report (in English) as published by the Ministry is available here.

Starting today, and with the help of Microsoft, SLM Rijk offers zero exhaust settings to admins of government organisations. During the writing of this DPIA, Microsoft has committed to take a number of other important measures to lower the data protection

Improvement measures taken by Microsoft

Between **April and June 2020**, SLM Microsoft Rijk and Microsoft agreed on measures to mitigate the six high data protection risks for Office for the Web and the mobile Office apps. As agreed, and verified by Privacy Company, since 1 August 2020, Microsoft had implemented 4 mitigating measures. These were:

1. Provide further information on the third parties identified in the DPIA report and classification of these parties either as a sub-processor (if Microsoft is a processor) or a Controller Connected Experience, a Non-Microsoft Product or an Add-In (if Microsoft is the controller).
2. Roll out controls by which the system administrator can limit or turn off, at the customer's choice, the use of optional/Controller Connected Experiences for the Excel, OneDrive, Outlook, PowerPoint, Teams and Word mobile applications.
3. Roll out controls to limit the collection by Microsoft of Diagnostic Data from the Excel, OneDrive, Outlook, PowerPoint, Teams and Word mobile applications (telemetry limitation choice for admins), plus ensure that all Diagnostic Data collected from Office for the Web will be limited to (the minimum level of) *Required Service Data*.
4. Prevent the presence of certain content (file-, pad-, usernames) in Telemetry Data when using parts of Office for the Web.

In **February 2022**, Microsoft was provided with this updated DPIA report. Microsoft confirmed the findings, and suggested some factual corrections. For example: the EU Data Boundary will be applied by default to all EU Enterprise and Education customers, and does not require an active opt-in from the admins. Microsoft referred to a public

Real world impact: A few examples

2

Outcome: ten high data protection risks

The outcome of this DPIA is that there are ten high data protection risks and three low data protection risks. The high risks, and mitigating measures, are shown in the table at the end of this summary.

DPIA Google G Suite Enterprise

Data protection impact assessment on the processing of personal data on 3 platforms with the Chrome browser and as installed apps

Version 1 – for consultation with the Dutch DPA

Date	9 July 2020, with update on 12 February 2021
Status	Public

The Register

Off-Prem ▸ SaaS

Dutch public sector gets green light to use Google Workspace

Data Protection Impact Assessment merely a 'standard step'

Richard Speed
Mon 30 May 2022 // 14:15 UTC

Google Cloud's managing director for Benelux, Joris Schoonis, said: "This is a milestone for Google Cloud's relationship with the Central Dutch Government, ***as we see the results of the DPIAs come to fruition***"

DPIA IN AFRICAN REGIONAL, SUB-REGIONAL AND NATIONAL INSTRUMENTS

DPIA in African regional and sub-regional instruments

	African regional and sub-regional instruments on data protection	DPIA Provision
1	African Union Convention on Cyber Security and Personal Data Protection 2014	None
2	Supplementary Act A/SA. 1/01/10 on Personal Data Protection within ECOWAS (February 2010)	None
3	Southern African Development Community (SADC) Model Law Data protection (recognizes the risk-based approach in the security obligation, but does not explicitly provide for DPIA)	None
4	African Commission on Human and Peoples' Rights Resolution 362 (LIX) on the Right to Freedom of Information and Expression on the Internet in Africa	None

DPIA in African regional and sub-regional instruments

	African regional and sub-regional instruments on data protection	DPIA Provision
5	African Commission on Human and Peoples' Rights Declaration on Freedom of Expression and Access to Information in Africa 2019 (65th Ordinary session)	None
6	African Declaration on Internet Rights and Freedoms	None
7	Personal Protection Guidelines for Africa 2018	None
8	The AU Digital Transformation Strategy for Africa (2020-2030)	None

DPIA in national instruments

	Country	Data Protection Instrument	Provision on DPIA	Remarks
1	Kenya	Data Protection Act 2019	Section 31 (1)	Explicit requirement
2	Mauritius	Data Protection Act 2017	Section 34	Explicit requirement
3	Ghana	Data Protection Act 2012	Section 28	Implied requirement
4	Lesotho	Data Protection Act 2011	Section 20	Implied requirement
5	Malawi	Data Protection Act 2022	Section 24	Explicit requirement
6	Nigeria	Nigeria Data Protection Regulations 2019 NDPR Implementation Framework 2020	Article 4.1(5) Para 3.2(viii), 4.2	Implied requirement Explicit requirement
7	Rwanda	Law relating to the protection of personal data and privacy, N° 058/2021 of 13/10/2021	Article 38	Explicit requirement
8	South Africa	Protection of Personal Information Act 2013 Regulations Relating to the Protection of Personal Information (2018)	Section 19 Section 4	Implied requirement Explicit requirement
9	Uganda	Data Protection Act 2019 Data Protection and Privacy Regulations, 2021	Section 20(2) Section 12	Implied requirement Explicit requirement
10	Zambia	Data Protection Act No. 2 of 2021	Section 46	Explicit requirement

DPIA in national instruments

	Country	Data Protection Instrument	Provision on DPIA	Remarks
12	Zimbabwe	Data Protection Act No. 5 of 2021	Section 20, 21	Implied requirement
13	Morocco	Law No. 09-08 Deliberation No. D-188-2020 of 14 December 2020	No Provision Page 3 of the DPIA Deliberation	Morocco is a party to Convention 108+ Recommends DPIA
14	Benin	Law No. 2009-09 of May 22, 2009, Dealing with the Protection of Personally Identifiable Information (Law No. 2009-09)	Section 50	Implied requirement
15	Ivory Coast	Law 2013-450	No provision	However, ARCTI is beginning to impose it as a good practice for processing sensitive data
16	Cape Verde	Law No. 121 /IX//2021 (amendment to the Law No. 133-V-2001)	Article 16-D	Express requirement
17	Republic of Congo	Law 29-2019 on the Protection of Personal Data	Art 79	Explicit requirement
18	**Tunisia; Burkina Faso; and Senegal**	**Obligation as parties to Convention 108+**	**Article 10 (2)**	**Explicit requirement**

DPIA FRAMEWORK: THE KENYAN EXAMPLE

Kenyan development on the right to privacy and DPIA

I. Independence Constitution 1963
II. Constitution of Kenya 2010 - Article 31
III. 2010-2019: Courts and legal development
IV. Data Protection Act 2019 - Section 31 on DPIA
V. Additional influence by courts (*Nubian Rights Forum & Katiba Institute* cases)
VI. Data Protection Regulations 2021
VII. Guidance Note on Data Protection Impact Assessment 2022
VIII. Advisory on Data Impact Assessment
IX. Other Codes on DPIA procedures and processes (financial sector, political parties)

Key Legal Development on DPIA

30 January 2020 Ruling - Nubian Rights Forum case

The Hight Court briefly commented on the new Data Protection Act having come into force roughly a month before the judgment, noting that it was not enough to just have a data protection legal framework in place, but that "once in force, data protection legislation must also be accompanied by effective implementation and enforcement" and "adequate protection of the data requires the operationalisation of the said legal framework"

14 October 2021 Ruling - Katiba Institute case

The High Court declared the collection of biometric information and the rollout of the Kenya's digital ID system "*Haduma cards*" unconstitutional, citing the disregard of data protection frameworks, including the failure to conduct a data protection impact assessment as required by the Kenyan Data Protection Act of 2019 (Art. 31).

- Although the roll-out of the mass collection of personal data under the National Integrated Identity Management System took place in March 2019, before the Kenyan Data Protection Act (DPA) came into force on 25 November 2019, the High Court ruled that the DPA applied retrospectively

- The High Court issued an order compelling the government to conduct a data protection impact assessment in accordance with Section 31 of the Data Protection Act before continuing to process data and rolling out the Huduma Namba cards

Key attributes of the Kenyan DPIA framework

- DPIA is an explicit obligation (Art 31)
- The ODPC has issued further guidelines and regulation on how to conduct a DPIA
- There is blacklist and whitelist of operations requiring a DPIA
- Consideration of risks to rights and freedoms of the data subject

Key attributes cont.

- Embeddedness on self-regulation and meta-regulation
- Emergence of internal and industry-specific regulations
- Court as a key norm developer

Areas for Improvement

- Insufficiency of the DPIA Template
  - ✓ Understanding the DPIA Template within the context of international best practices

- Lack of a stakeholder engagement procedure in DPIA process
  - ✓ Consultation should include crucial actors including data subjects

- DPIA reporting framework

CONCLUDING REMARKS: LESSONS FOR AFRICA

CONSIDER DPIA INCLUSION IN SUBSEQUENT REGIONAL AND SUBREGIONAL INSTRUMENTS

- Surprisingly, none of the major data protection instruments at the African Regional/sub-regional levels considered DPIA which the Kenyan High Court regarded as a crucial component of accountability and relied upon to enforce the constitutional right to privacy and data protection
  - Cf, the IBA African Regional Forum Data Protection/Privacy Guide for Lawyers in Africa

❖ It is recommended that subsequent amendments to these instruments or new ones should include a DPIA mechanism

AUTHORITIES IN AFRICA SHOULD USE THIS TOOL PROACTIVELY

- In the case of a digital ID system, DPIA must prior to deployment of such systems be carried out and the outcome should inform the decisions on the design, implementation, and safeguards of such digital ID systems

- Existing systems and framework should proactively be assessed, emulating the Dutch authorities

HARNESS CURRENT DEVELOPMENTS TO AFRICA'S ADVANTAGE

- Several approaches/tools exit including:

❑ From ISO and other standards

- ✓ ISO 31000:2018 Risk management – Principles and guidelines (Generic tool)
- ✓ ISO 29134:2017 Guidelines for PIA
- ✓ NISTIR 8062 Privacy Engineering and Risk Management in Federal Systems

❑ DPA Guidelines: EDPB, ICO, CNIL, AEPD, etc.

❑ CNIL software tool

❑ Academic publications

- ✓ Privacy Impact Assessment edited by David Wright, Paul Hert
- ✓ Privacy RIsk Analysis Methodology (PRIAM)
- ✓ SDM

Thank You

nwankwo@iri.uni-hannover.de

Nelson.Okeyo@fau.de