

World Bank's Symposium on
Building DPI
ecosystems that
people can trust

ID4Africa AGM
May 15th, 2026
Abidjan (Côte d'Ivoire)



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)



Index

1

Presentation: Trusted Data for Trusted DPI

2

Panel Discussion: Ensuring Accountability: The Role of Regulators and DPAs

3

Fireside Chat: From National to Regional Frameworks

Symposium Facilitator



Mateo GARCÍA SILVA

Digital Specialist, World Bank





Trusted Data for Trusted DPI

DPI Data Risks and Safeguards
across the Data Lifecycle

Presented by:

Prakhar BHARDWAJ
Digital Safeguards Specialist
World Bank

**Dr. Zhijun William
ZHANG**
Lead, Cybersecurity
World Bank



Trusted Data for Trusted DPI



Prakhar BHARDWAJ

Digital Specialist, World Bank



Dr. Zhijun William ZHANG

Cybersecurity Lead, World Bank





Meet Amina ...



Amina, 34, is a market trader in Niamey, Niger. She sells vegetables and dried goods to support her three children.

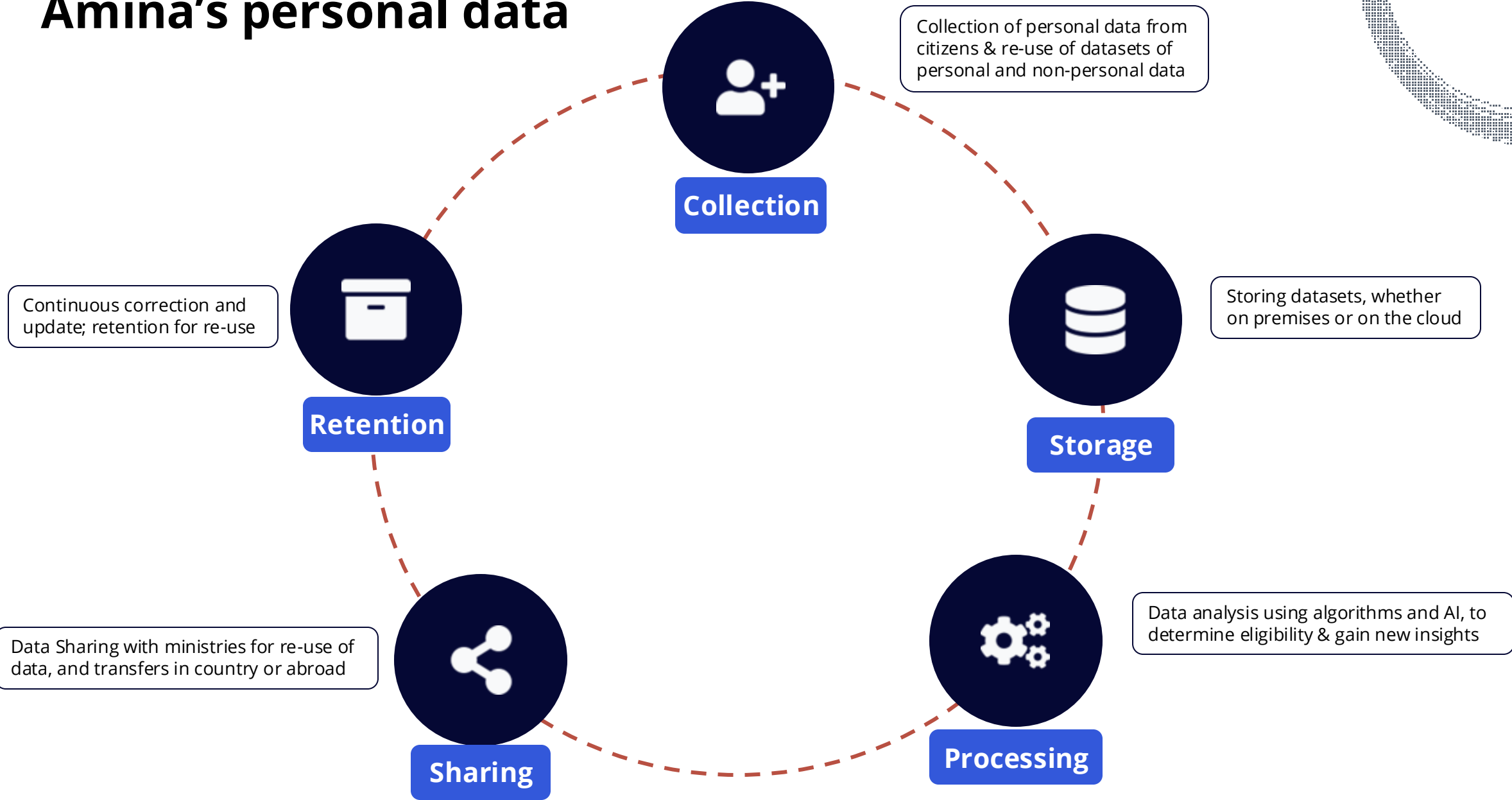


When her government launched a digital social protection programme, she wants to enroll hoping the monthly cash transfer covers some part of school fees and food expenses.





The data lifecycle helps us understand the journey of Amina's personal data



Amina has many apprehensions as she decides to enrol

01

What if Amina's neighborhood in Niamey, Niger gets left out of the enrollment drive?

02

What if Amina's personal data, like her fingerprint, is captured inaccurately or incompletely?

03

Does Amina truly understand what she is 'consenting' to?

04

If so, does she have the capacity to say no? and opt out?

05

Does she understand that her personal data will probably be used by the Government for other schemes?

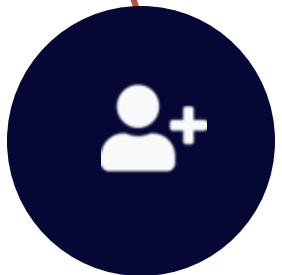
06

Can she ask someone these questions? Find recourse if she faces an injustice?





Unfortunately, some of her apprehensions turn out to be true ...



Collection



"No ID, No Service!"

Denial of service due to details and ID not matching

Overcollection of personal data

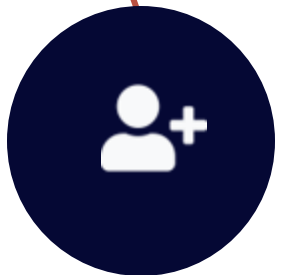
Compelled disclosure of personal data

Possibility of oversharing and reuse of data leading to harm

Lack of recourse or oversight



It wasn't the first time a citizen suffered due to weak safeguards at point of data collection



Collection

Kenya: Huduma Namba

Legal non-compliance

- **What happened:** 36 million people enrolled and 10 million biometric IDs issued (2019–2021)
- **What went wrong:** No Data Protection Impact Assessment was conducted before rollout
- **Impact:** High Court ruled the program illegal; Ksh 10 billion spent and entire rollout reversed

India: Aadhar

Exclusion by design

- **What happened:** Biometric authentication failed for up to 49% of users in Jharkhand and 37% in Rajasthan
- **What went wrong:** In 2017, 33% of Aadhaar-linked ration card holders in Rajasthan could not access food rations
- **Impact:** Millions denied essential benefits; failure rates have since improved after major reforms

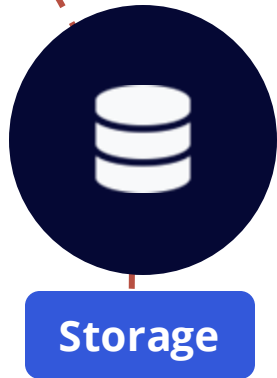
Uganda: Digital ID

Access denied

- **What happened:** Since 2019, national ID required to access public health facilities
- **What went wrong:** No alternative for citizens without ID documents
- **Impact:** Patients turned away from essential healthcare for lacking ID



Storage of citizens data, whether on-prem or in the cloud, also exposes it to a new set of risks



- 01** *Weak or Inconsistent cybersecurity standards amongst different vendors*
- 02** *Single Points of Failure*
- 03** *Data Proliferation leading to multiple “weakest links”*
- 04** *Lack of comprehensive cryptography and encryption*
- 05** *Weak SOC for DPI system or CSIRT*
- 06** *Lack of Incident Reporting and Emergency Response and Preparedness*





Unfortunately, one 'weak link' is all it takes for a breach



Storage

Bangladesh: Registrar General

Infrastructure failure

- **What happened:** Personal data of 50+ million citizens exposed through a government website (2023)
- **What went wrong:** Weak infrastructure left records publicly accessible; a researcher found them via a Google search
- **Impact:** Names, addresses, phone numbers, and national IDs compromised; authorities unresponsive despite repeated alerts

Philippines: COMELEC

SQL injection

- **What happened:** Hackers defaced the COMELEC website and dumped voter datasets on public platforms (March 2016)
- **What went wrong:** SQL injection vulnerability allowed direct database access
- **Impact:** Names, addresses, birth dates, passport data, and fingerprints of millions exposed; called the largest government data breach at the time

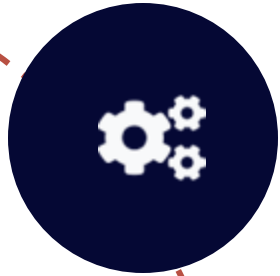
Brazil: Ministry of Health

Credential exposure

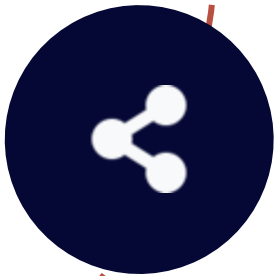
- **What happened:** Database credentials left in website source code for six months; ransomware attack followed in Dec 2021
- **What went wrong:** Passwords stored in easily decoded Base64 in public source code; weak cybersecurity practices
- **Impact:** Medical records of 243 million Brazilians leaked; COVID-19 vaccination data deleted (approx. 50 TB)



An algorithm wrongly assumed Amina was committing fraud



Processing



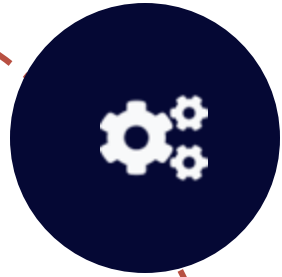
Sharing

- 01** A biased algorithm flagged Amina based on demographics with no reliability or explainability testing
- 02** No human review before action: the automated decision went straight to prosecution without any check
- 03** No right of appeal or accessible redress: Amina had no pathway to challenge the algorithm's verdict
- 04** Data collected for welfare was repurposed for fraud prosecution without consent or notice

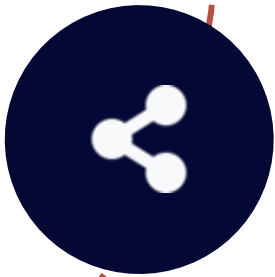




The incorporation of AI into personal data processing has heightened risks to citizens



Processing



Sharing

- 01** Algorithmic and AI Processing that reinforces biases and disproportionately impacts minorities
- 02** Data breaches by data processors due to improper cybersecurity practices
- 03** Cross-border data flows without enforceable oversight
- 04** Further transfers and processing beyond the original purpose

HOW THE FAILURE UNFOLDS

Citizen data enters the system



AI model processes data

Untested for bias or accuracy



Automated decision issued

Deny, flag, or restrict the citizen



No human review

No appeal pathway, no oversight

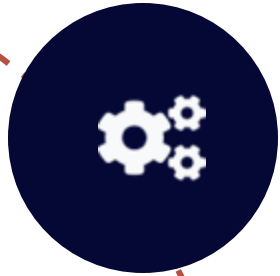


Harm to the citizen

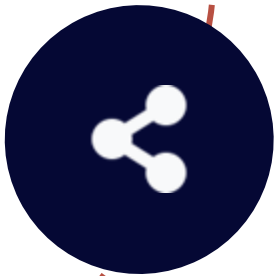
Exclusion, discrimination, loss of trust



Some cases where the lack of safeguards had a negative impact



Processing



Sharing

Netherlands: Childcare Benefits

(Toeslagenaffaire)
Algorithmic discrimination

- **What happened:** Tax authorities used algorithms to flag childcare benefit claims for fraud (2005–2019)
- **What went wrong:** “Foreign-sounding names” and “dual nationality” used as fraud indicators; self-learning system amplified bias with no human oversight
- **Impact:** Tens of thousands of low-income families falsely accused; ethnic minorities disproportionately targeted; government collapsed over the scandal

India: Aadhaar

Function creep

- **What happened:** Aadhaar launched as a voluntary ID for welfare delivery but was progressively linked to bank accounts, tax filings, phones, and over 500 government schemes
- **What went wrong:** Biometric data collected for one purpose was repurposed without meaningful consent; private companies gained access to authentication data originally meant for public services
- **Impact:** Supreme Court struck down mandatory linkages in 2018; exclusion of vulnerable populations from essential services due to biometric failures



Widespread adoption of AI worsens risks of algorithmic discrimination and oversharing of data

Sharing



Retention

- 01** Indefinite retention of data
- 02** Lack of pro-active correction and updating of data by government
- 03** Weak framework for citizens to correct or delete data
- 04** Combination, and reprocessing of data for other purposes
- 05** Weak endpoint security for government data bases, lack of incident response and reporting

HOW DATA ACCUMULATES

- Initial data collected**
Biometrics, ID records at enrollment
- Cross-linked across agencies**
Tax, health, social records merged
- Outdated data drives decisions**
Stale records, no correction mechanism
- Permanent digital shadow**
No erasure path, risk compounds indefinitely



Legal safeguards: Legislations and Program-level Safeguards

International best practices recommend a specific, enforceable, rights-based regulatory model for data governance.

Lawfulness and Transparency in Data Collection

Lawful bases for processing defined in statute. Data collection subject to principles of purpose limitation, data minimization, and proportionality.

Basis for Onwards Transfer & Sharing circumscribed

Non-consent basis of sharing personal data must be limited to specific, narrow grounds.

Data Transfers Regulated at Home & Abroad

A data governance framework that logs intra-governmental data transfers; and an enforceable cross-border data transfers regime.

Enforceable Individual Rights

Statutory pathways to challenge automated decisions. Right to human review of consequential outcomes.

Independent Supervisory Authorities

SOC monitoring, 72-hour incident notification, and clear allocation of risk management responsibility & a strong, independent DPA



Institutional Safeguards: Multi-Level Stakeholders

01

Oversight at the Organizational Level

- Data Protection Officers
- CISOs
- Sector regulators — domain-specific oversight (health, finance, telecoms).

02

Independent oversight & redress

- Oversight bodies with real investigatory and enforcement powers.
- Accessible correction and complaint pathways for citizens.
- Public reporting of compliance and incidents.

03

Cooperation under stress

- ID Authorities, DPI stakeholders, and the national CSIRT must cooperate before a crisis, not during one.
- Government-wide or ID-specific Security Operations Centers (SOC) for rapid detection at scale.
- Tested incident-response and continuity playbooks.



Technical & operational safeguards — and a return to the citizen



1

Privacy & security by design

Data minimization, least privilege, and privacy-by-design embedded in system architecture and procurement contracts — not bolted on after launch.

2

Cybersecurity controls

Tokenization, multi-factor authentication, role-based access controls, encryption in transit and at rest, comprehensive logging — the baseline of confidentiality, integrity, and availability.

3

Secure interoperability

Standards that enable trusted sharing across borders and between agencies — while enforcing data accuracy, retention compliance, and full auditability of every access.

THE CITIZEN, RETURNED

*When law, institutions, and architecture work together, the widow's thumb still does not match — but the system has a fallback. **Her pension arrives. Her trust holds.** That is the dividend of good DPI design — and it is the work of policymakers in this room.*



With the right safeguards, Amina's story ends differently

1

Legal protection at enrollment

Data protection law limits collection to what is necessary. Amina gives informed consent and retains the right to challenge automated decisions.

2

Independent oversight & redress

A data protection authority monitors the system. Amina has clear, accessible pathways to file complaints and receive answers.

3

Privacy & security built in

Her biometrics are encrypted and tokenized. Fallback authentication means a failed scan never denies her services.

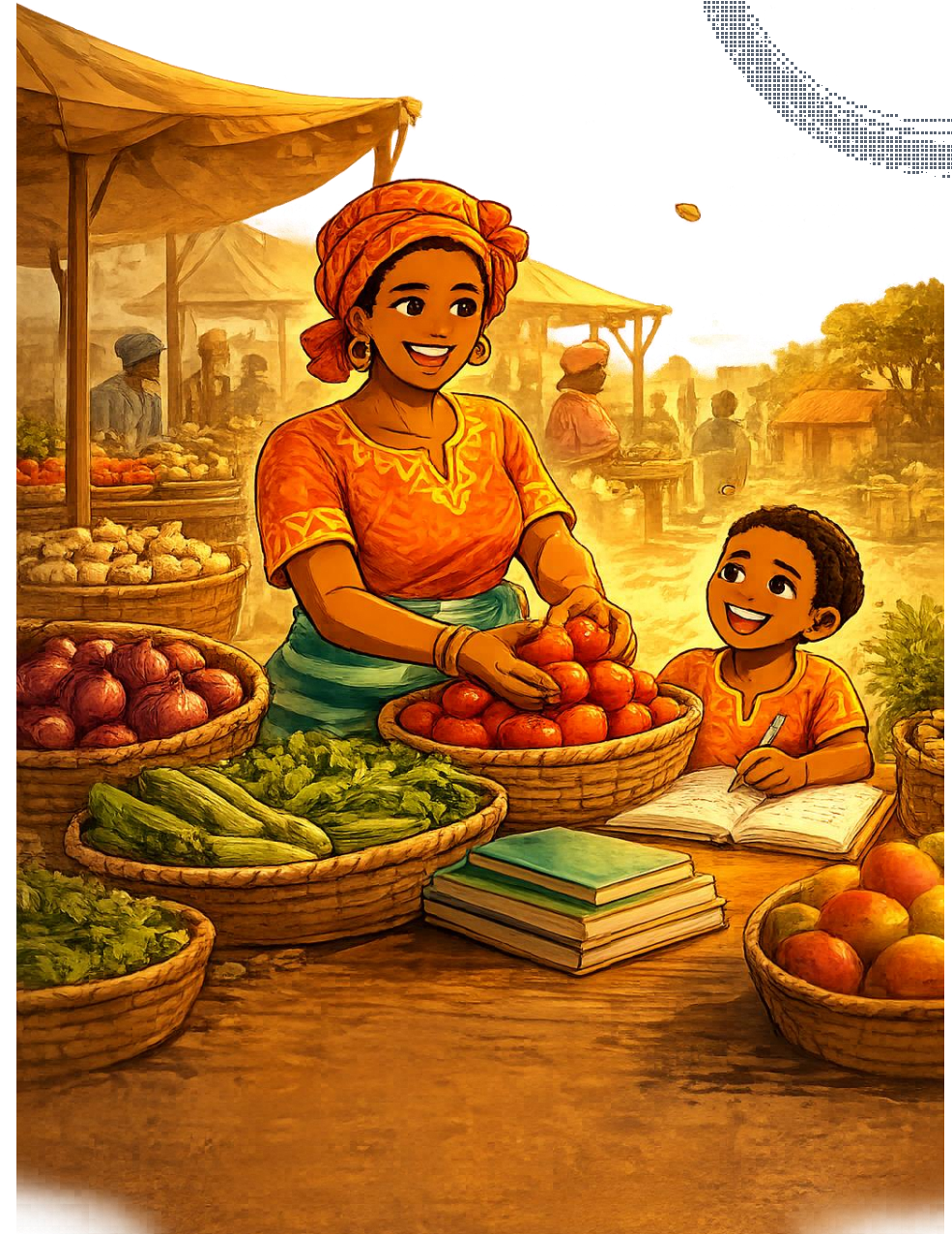
4

Governed sharing & retention

Her data stays within its original purpose, with full audit trails, defined retention limits, and enforceable deletion rights.

AMINA'S OUTCOME

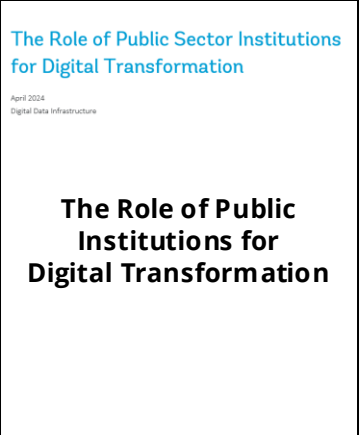
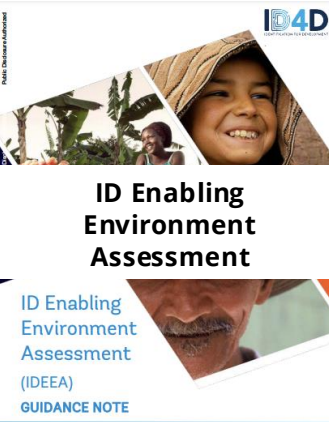
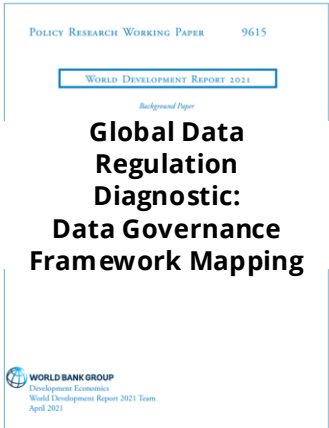
Amina enrolls with confidence. Her benefits arrive. When the system falters, it fails safely — and her trust in the state holds.





Global Resources for Data Protection and Adjacent Topics

Current World Bank Guidance



Forthcoming Guidance

Title	Description
Blueprint for Data Protection Authorities (DPAs)	Defines institutional mandates, enforcement mechanisms, and governance structures.

Toolkit for Data Protection in Digital Ecosystems without a DP Law	Offers a structured approach for establishing interim safeguards in the absence of dedicated legislation.
---	---

Cheat-sheets for EU Data Regulations	Regulatory steps and compliance essentials for AI Act, Data Governance Act, Data Act; GDPR.
---	---

Practitioners' Note on Cross-Border Data Flows	Addresses regulatory fragmentation and interoperability challenges.
---	---




DPI

ID4D
Knowledge

**Technical
Guidance**

id4d.worldbank.org

Trust Services

https://bit.ly/WB_eSig



https://bit.ly/WB_PKI

Q&A

Ensuring Accountability: The Role of Regulators and DPAs

Moderator



Taylor REYNOLDS

*Global Practice
Manager, Policy &
Regulations Digital & AI
The World Bank*

Panelists



Lorpu PAGE

*Executive Director,
Independent Information
Commission (IIC), Liberia*



**Luciano
HOUNKPONOU**

*Chairman, Autorité de
Protection des Données
(APDP), Benin*



**Drudeisha
MADHUB**

*Data Protection
Commissioner, Data
Protection Office (DPO),
Mauritius; and President,
Francophone Association
of Personal Data
Protection Authorities
(AFAPDP)*



Adamou IRO

*President, High Authority
for Personal Data
Protection (HAPDP),
Niger; and President,
African Network of
Personal Data Protection
Authorities (NADPA-
RAPDP).*



Fireside Chat

Moderator



Mateo GARCÍA SILVA

*Digital Specialist,
World Bank*

Panelist



Rose MOSERO

*Data Protection and
Cybersecurity
Advisor, East African
Community (EAC)*



**Thank you very
much!**

ID4Africa AGM
May 15th, 2026



WB Team

For queries or comments, please contact:



Taylor REYNOLDS
Global Practice
Manager, Policy
and Regulation,
Digital & AI VPU
The World Bank



**Dr. Zhijun William
ZHANG**
Cybersecurity Lead,
Digital & AI VPU
The World Bank



**Prakhar
BHARDWAJ**
Digital
Development
Specialist,
Digital & AI VPU
The World Bank



**Mateo GARCÍA
SILVA**
Digital
Transformation
Consultant,
Digital & AI VPU
The World Bank