2nd African Forum on Cybercrime

28-30 June 2021

Data Protection legislation as enabling factor for digital innovation plans

Sanusi Drammeh
Principal ICT Officer
MINISTRY OF INFORMATION & COMMUNICATION INFRASTRUCTURE
THE GAMBIA

COUNCIL OF EUROPE

EUROPEAN UNION

CONSEIL DE L'EUROPE

Outline

- Data Protection & Privacy
- Digital Innovation
- Data Protection correlation with Digital Innovation
- Enabling Factors
- Statistics
- Conventions & Treaties
- Case Studies
- Way forward
- References

Data Protection & Privacy

Definition

- Data Protection and Privacy is ensuring:
  - the protection of any information relating to an identified or identifiable individual (“data subject”)
  - irrespective of nationality or residence, with regard to the processing of such information
  - thereby contributing to respect for the individual’s human rights and fundamental freedoms, and in particular the right to privacy.

Digital Innovation

Definition

- Digital Innovation is the use of digital technology and applications:
  - to improve existing business processes and workforce efficiency,
  - enhance customer experience,
  - and launch new products or business models

Digital "Innovation" as a Pillar of Digital Transformation

- Six Pillars of Digital Transformation
  - experiences,
  - people,
  - change,
  - <u>**innovation,**</u>
  - leadership,
  - culture

Innovate → Transform

Digital Innovation Vs Digital Transformation

- Digital transformation is an ongoing process to transform and improve business performance
  - by changing the way a company thinks and operates.
  - Unlike common perception, digital transformation isn’t only about the technology you adopt, but also involves people, process, and portfolio.

- Digital innovation is that spark of creativity that leads to development of new technology or innovative applications of existing digital technology.
  - Digital innovation is often the precursor to digital transformation.

Digital Innovation examples

- wearable devices,
- chatbots,
- Internet of Things,
- Artificial Intelligence,
- big data

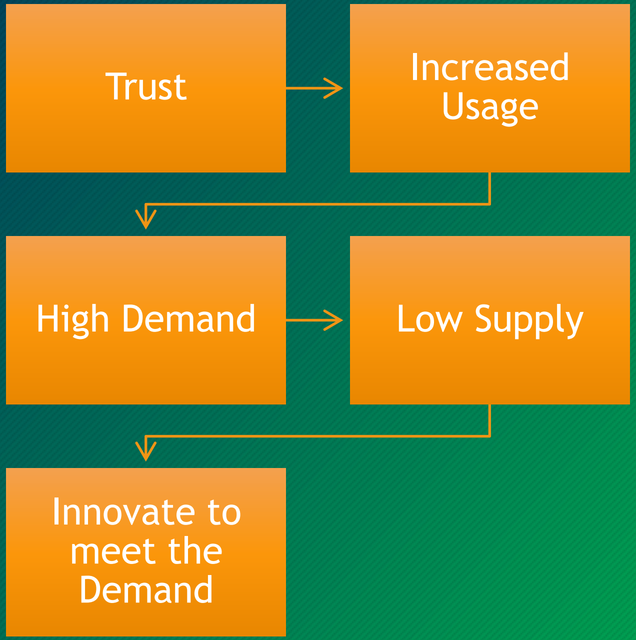
Data Protection correlation with Digital Innovation

- Innovation spurs delivery of new “Technology”
- “Technology” is required to ensure:
  - Effective and efficient Protection - during processing of personal data
  - Privacy – confidentiality of information being processed/controlled
  - Enforcement legislation and regulatory frameworks for monitoring/oversight
  - Investigations and delivery of admissible evidence

Enabling Factors

1. Consumer Trust & Confidence

- **Presence of Data Protection laws** can inherently improve trust and confidence of data subjects when using technologies that data processors or controllers provide because of existence of:
  - laws that provides their rights and responsibilities
  - regulations that governs service providers
- (digital) Trust & Confidence is an essential factor that drives innovation. When there is trust the demand for digital services will be high. The higher the demand, less the supply, which will require innovation to meet demands.



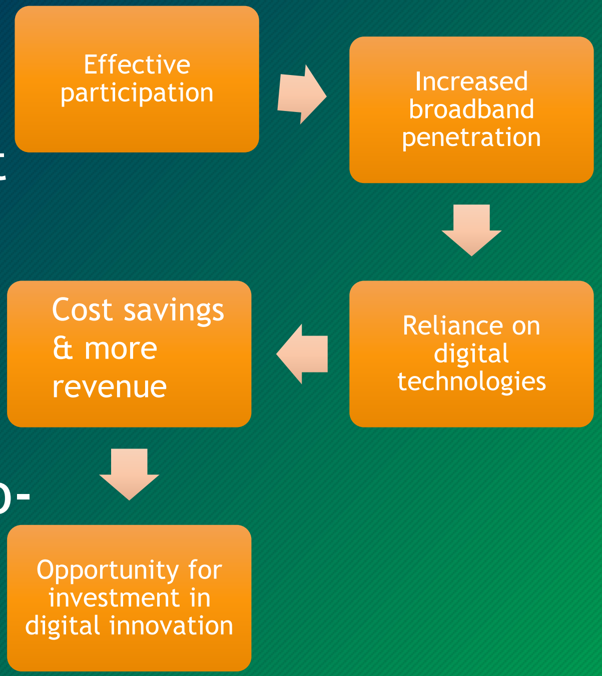
2. Increased & effective participation in the usage of Digital technologies

- Factor 2 is complementary to Factor 1 (Consumer Trust & Confidence)
- When "Trust & Confidence" is bestowed on digital system:
  - data subjects or people feel more and more comfortable to use digital systems, resulting in an increase participation in the utilization of digital technologies.
  - Also, accelerating growth for both people and entities. That means more money and more investment into digital innovation.

Increased Usage → Increased revenue → Investment → Digital Innovation

3.Economic growth & Development

- Because of the digital trust and confidence, Data Protection & Privacy legislations may influence:
  - effective participation of people in the usage of digital technologies,
  - increased broadband penetration.
  - increased reliance and drastic reduction on the usage of manual and inefficient processes to conduct transactions.
  - Cost savings and more revenue
  - Opportunity to Invest in digital innovation to ensure competitive edge



- It is evident that a nation that heavily utilizes reliable, secure and available digital technologies on a day-to-day basis will experience socio-economic development.
  - According to a World Bank study, it is estimated that for every 10% increase in broadband penetration in low and middle income countries result in a commensurate increase of 1.38% of the GDP

4.Accountability and Transparency

- Accountability:
  - Ensures responsible behavior in the digital market
  - The digital ecosystem is forced to play catch-up by innovating new technologies in order to adhere to legal obligations.
- Transparency:
  - Consent of data subjects regarding the processing or control of their personal information. Technology can help enhance this processes.
  - Visibility (also dependent on technology) of the control and processing of personal information of data subjects.

Responsible behavior

Innovation & Adherence to legal obligations

Consent Driven and Visibility

5.Complaince

- In order to survive the market, data processors and controllers are obligated to abide by the law.
- When there is compliance, consumer trust is even more invigorated and customer bases tend to increase.
- To stay a competitive edge, data processors and controllers would need to adopt or innovate new technologies (such as implementing safeguards – to prevent cyber threats)

6.Consumer Protection

- Factors 1,2,4 & 5, the rights of Consumers of digital technologies are protected.
- Consumer protection is fundamental to digital innovation because technology innovators take into account standard best practices that may be required or premised from legislations to ensure compliance in processing or controlling personal data.

7.Research & Development

- Within existing provisions in data protection regulations such as those borrowed from Convention 108+ or AU Malabo Convention gives exceptions for research purposes.
- These exceptions provide an opportunity for technology innovation by collecting data necessary for research and development.

Research AI
- data
- data

Research Big Data
- data
- data

Research Wearable Devices
- data
- data

8.International Cooperation

- To ensure effective cooperation with countries, it is essential to harmonize laws on data protection legislations. This will ensure:
  - Sharing Best Practices
  - Providing Mutual Assistance
  - Providing Technical Assistance
  - Effective Regulation of trans-border data
- Harmonization through international cooperation can yield prospects of innovating new technologies to protect trans-border data flows.

Conventions & Treaties

AU Agenda 2063

- The Africa We Want:
  - envisions Africa as a continent on equal footing with the rest of the world
  - as an information society, an integrated e-economy
  - where every government, business and citizen has access to reliable and affordable ICT services
  - by increasing broadband penetration and providing venture capital to young ICT entrepreneurs and **innovators.**

AU Agenda 2063 - DIGITAL TRANSFORMATION STRATEGY FOR AFRICA (2020-2030)

- Enabling Environment, Policy & Regulation, Policy Recommendations And Proposed Actions:
  - “Integrate the provision of eServices, developed by both the public and private sector, with adequate legal acts and regulation at all levels, ensuring that data needed to provide eServices for the community is openly available while fully respecting data protection rights.”

Sub-Actions

- Allow relevant organisations in Member States or Region Economic Communities to reuse core registers and **information systems from other organisations in a secure data exchange environment, enabling the different information systems and registers to communicate, share data and work together (requires innovation)**

- Better use of data for better decision-making around policy and regulation. Data driven decision-making implies systematic collection and assessment of market data (both supply and demand) to inform regulation and guide policy priorities. In addition to the system itself, policymakers and regulators require clear measurement frameworks and the technical capacity to monitor data

AU Malabo Convention – Cybersecurity & Personal Data Protection

- The AU convention objective is setting the essential rules for establishing a credible digital environment (cyber space) and address the gaps affecting the regulation and legal recognition of electronic communications and electronic signature; as well as the absence of specific legal rules that protect consumers, intellectual property rights, personal data and information systems and privacy online.

AU Malabo Convention cont.

- Outline:
  - PART II: Personal Data Protection
  - Section I : Personal Data Protection
  - Section II : Institutional framework for the protection of personal data
  - Section III : Obligation relating to conditions governing personal
  - data processing
  - Section IV : The Data Subject Rights
  - Section V : Obligation of personal data controller

AU Malabo Convention Cont.

- Senegal, Guinea , Mauritius and Ghana have ratified the Malabo Convention and so far nine (09) Countries have already signed : Benin, Tchad, Comoros , Congo, Guinée Bissau, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia.

  -2018 report.

Convention 108+ (Convention for the protection of individuals with regard to the processing of personal data

- Opened for signature on 28 January 1981
- First legally binding international instrument in the data protection field.
- Parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to processing of personal data.

Convention 108+ cont.

- 8, November, 2001 – required parties to set-up independent supervisory authorities
- 2013, Accession of the first non-European State, Uruguay to the Convention.
- 2018 – Amended protocol CETS No. 233 – modernization of Convention 108.
- Present – 55 State parties to Convention 108+

ECOWAS Supplementary Act on Personal Data Protection & Privacy

- Signed by ECOWAS Heads of States:16th Day of February 2010

CHAPTER II - LEGAL FRAMEWORK FOR PERSONAL DATA PROTECTION:

Article 2: Aims

- Each Member State shall establish a legal framework of protection for privacy of data relating to the collection, processing, transmission, storage, and use of personal data without prejudice to the general interest of the State.

Statistics

Statistics

- According to a World Bank study, it is estimated that for every 10% increase in broadband penetration in low and middle income countries result in a commensurate increase of 1.38% of the GDP
- Although Africa makes 16% of the world population, its GDP share to the global economy only amounts to 5% (IMF, 2019)
- The AfCFTA will be a market of 1.2 billion consumers, which will reach 1.7 by 2030 with a combined GDP of 2.1 to 3.4 trillion US dollars, depending on sources of data. In addition, Africa's current private and business to business consumption is estimated at US$4.0 trillion. Intra-African trade is expected to increase by 52.3% by 2022 and double if there is effective elimination of Non-Tariff Barriers. Digital trade will play a key role in boosting intra-African trade.

Absence of a Data Protection Legislation & effects

- Lack of Trust and Confidence in the usage of digital technologies
- Cybercrime will increase with the absence of appropriate safeguards to protect personal data of individuals.
- Exploitation or breach of Consumer rights
- Fraud theft and sales of PIIs
- No accountability or transparency
- Illegal trade (Dark Web) or illegal business practices
- Less international cooperation in practical terms
- Stifling of innovation
- Unregulated sector resulting in “Digital Mob-Justice”

Case Studies

The Gambia Data Protection Legislation

- First legislation was part of the Information Communications Act of 2009
  - Deficiencies in the act which was not very comprehensive
- 2019 – Data Protection formulation began and was adopted in 2020
  - Supported by CoE
- 2020 – Compressive separate Data Protection Bill was drafted and validated
  - Supported by CoE

Way forward

Way forward

- Adoption of international best practices
- Signing and ratification of treaties and conventions
- Development and adoption of standards at regional and domestic levels relating to data protection and privacy for service providers, vendors/manufactures/innovators.
- Clearing misconceptions on data protection as stifling revenue generation for businesses
- Awareness raising and sensitization
- Mutual and equitable assistance without additional laws causing barriers to cooperation.
- More international cooperation and sharing of best practices
- Improve and strengthen capacity building approaches

References

1. 2 Kim, Y., Kelly, T., and Raja, S. (2010). Building broadband: Strategies and policies for the developing world. Global Information and Communication Technologies (GICT) Department, The World Bank, January 2010
2. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf
3. Microsoft Word - E_AU Convention on CyberSecurity & Pers. Data Prot (opennetafrica.org)
4. Supplementary Act on Personal Data Protection within ECOWAS • Page 1 • ICT Policy Africa
5. AU Agenda 2063 Strategy 2020-2030