Table of Contents

Data Protection Impact Assessment (DPIA) Report

Project Title: Implementation of Biometric Attendance System at Nususi IT Consulting

Date: July 2025
Prepared by: Tania Bwari

1. Introduction

Nususi is an IT Consulting services company that intends to implement a biometric system using fingerprint/ face recognition scanners in their head office premises in Nairobi. This DPIA aims to evaluate the potential privacy impacts, identify risks of processing PII and recommend measures to ensure compliance with the 2018 Kenya Data Protection Act and applicable international standards including GDPR

2. Purpose of Processing

The biometric data processed by the system will be used to:

- Enrolment of biometric templated
- Accurately record staff attendance to eliminate buddy punching and time fraud
- Restrict and allow access to different areas of the organization
- Secure storage and deletion of biometric data based on company retention policy

Assessment of Necessity & Proportionality

- Necessity – Address security needs in sensitive zones like server rooms. Biometrics provides higher accuracy and prevents fraudulent attendance.
- Alternatives
    - RFID – Loss/ theft/buddy punching)
    - PIN – Less secure and shareable

3. Data Flow and Scope

Data Subject: Nususi Employees including contractors, interns and permanent staff, Vendors and visitors with temporary access, customers.

Data Collected: Fingerprint/ facial recognition biometric data, User IDs, Timestamps, Names, Department.

Storage: Encrypted local server with scheduled backups to AWS Cloud

Access: Restricted to HR Team, authorized IT personnel, authorized physical security personnel

4. Legal Basis for Processing

- **Legitimate Interest**: For access control and attendance management

- **Consent**: Due to the sensitive nature of biometric data
- **Stakeholder Engagement:**
  - **HR –** System use and enforcement
  - **IT –** Technical implementation and security
  - **Legal –** Compliance and contractual issues
  - **Employees –** Feedback and transparency

5. Risk Assessment

Risk	Likelihood	Impact	Risk Level	Mitigation
Inadequate consent policies and procedures	High	High	High	• Design clear policies around processing PII • Design clear and informed consent forms • Opt-out provisions
Unauthorized access to biometric data	Medium	High	High	• Data Encryption • Authentication and Authorization Mechanisms • Role based access controls • Data Categorization
Data loss	Low	High	High	• Backup policies • Endpoint protection • IR and DRP Plans • Regular backups • Regular vulnerability scans
System Failure / Lockouts	Medium	Low	Medium	• Redundant systems • Manual overrides
Function creep – Use of data beyond intended use	Low	High	High	• Policy enforcement • Guidelines to limit data use
Poor third party controls	Medium	Medium	Medium	• Conduct due diligence • DPA legal agreement
Misuse of personal data	Medium	High	High	

6. Applicable Legisislative Framework

Processing of personal data in Kenya is governed by the Constitution and other legislations which include but are not limited to the following.

a. **The Constitution of Kenya, 2010 Article 31 (c) and (d)**

Guarantee the right to privacy with regards to their information or that relating to their family or private affairs unnecessarily required, revealed or infringed. Article 35 states that every citizen has the right to information held by another person and required for the exercise or protection of any right or fundamental freedom. Further, every person has the right to the correction or deletion of untrue or misleading information that affects the person.

b. **The Data Protection Act, No. 24 of 2019**

It identifies certain types of personal information as more sensitive and offers them additional protection, establishes the Office of the Data Protection Commissioner and further provides for the protection of personal data and privacy of individuals in Kenya, including the data processed across jurisdictional borders.

c. The Computer Misuse and Cybercrime Act, No. 5 of 2018

The Computer Misuse and Cybercrimes Act safeguards the confidentiality, integrity, and availability of computer systems, programs, and data. It establishes legal protections against cyber threats by criminalizing malicious activities targeting individuals using computer systems, as well as attacks directed at computer systems themselves.

d. The Elections (Technology) regulations of 2017

Defines biometrics as unique identifiers or attributes, including fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves and DNA.

e. Digital Health Act, No.15 of 2023 The Digital Health Act, No. 15 of 2023

Establishes a legal framework for managing health data in Kenya, including the collection, storage, use, and protection of sensitive information such as biometric data.

7. Mitigation Measures

- Privacy by Design - Biometric data encryption at rest and in transit
- Periodic security audits – This is done to ensure compliance
- Transparency and Data Subject Rights – Clear and well drafted consent forms
- Data subject rights policy – Clear, documented and approved policies on the data subjects' rights concerning their data
- Retention and Storage Limitation -Data retention and destruction policy to ensure data is destroyed effectively without possibility of recovery and the data is not retained any longer than necessary.
- Purpose Limitation – Segregating data streams to ensure data is only used for function it was collected for

8. Approval and Monitoring

Approving Authority: DPO

DPO recommendations before implementation:

- Staff training on their rights as data subjects
- Proper consent is obtained
- Controls including technical, physical and administrative are verified and tested

9. Conclusion

The biometric system is justified for Nususi's security and operational needs, provided risks are mitigated via encryption, access controls, and transparency. Employee consent and compliance with local laws must be ensured before deployment.

Prepared by: Bwari Tania, DPO
Reviewed by: [DPO/IT Security Lead]
Approved by: [CEO/Compliance Officer]