DIGITAL PARKS AFRICA

PRIVACY POLICY

VERSION CONTROL

Document Number	*DPA-IMS-S-POL-00018*
Revision Number	*1*
Revision Date	*18/10/2023*
Issue Date	*18/10/2023*
Author	*Lynette Botha*
Approver	*Jacques De Jager*
Confidentiality Level	*Public*

T: +27 (0)12 004 0900 **E:** sales@dpa.host **W:** www.dpa.host
A: 1863 Cloud St, Louwlardia, Samrand, Centurion, 0157

CHANGE HISTORY

Date	Version	Created by	Description of change
18/10/2023	1	L Botha	First Issue

1. Overview

1.1 Purpose

The aim of this Policy is to:

- ensure compliance to the relevant privacy legislation/regulations for Digital Parks Africa operations inclusive of its data centre operations;
- educate the business on why the adherence to privacy legislation/regulation is important and the potential consequences of failing to comply; and
- inform the business of the procedures in place for dealing with any breaches that affect Digital Parks Africa Stakeholders.

1.2 Scope

This Policy is applicable to the following:

- All personal data / information including but not limited to customer information, Digital Parks Africa employees, third party and Digital Parks Africa company related information generated, processed and stored by operating companies at Digital Parks Africa to perform its activities and delivery of services;
- All systems and processes used in the course of managing personal data / information;
- Unless stated otherwise, this policy applies to all employees, contractors, and third-party personnel of Digital Parks Africa and operating companies accessing Digital Parks Africa information processing facilities. Digital Parks Africa information processing facilities include, but not limited to; Digital Parks Africa campuses, facilities, offices, work areas, secure areas, critical infrastructure rooms (CIR) and telecommunications rooms.

1.3 Audience

This policy applies to all individuals authorized to access Digital Parks Africa information processing facilities. This Policy is also applicable to the information that is handled and processed by contractors and third parties for Digital Parks Africa and Operating Companies.

1.4 Non-Compliance

Non-compliance with this policy must be reported to the Chief Executive Officer (CEO). Any breach may result in disciplinary action being taken, which may include dismissal.

Any disciplinary action arising from breach of this document will be taken according to the disciplinary code and grievance procedure of Digital Parks Africa. Where an employee is suspected of breaching the document, an internal investigation will be undertaken, depending on the outcome, civil and/or criminal legal action could be taken against the employee.

2. Policy Statements

2.1 Introduction

This policy addresses the requirements of legislation across different domains. As the legislation uses different terminology, for purposes of this policy the terms “Personal Data” and “Personal Information” have the same meaning and are used interchangeably.

Digital Parks Africa takes the Privacy of Sensitive and Personal Information of all its stakeholders seriously. Digital Parks Africa understands that sensitive and personal information is important to all stakeholders and is committed to protecting stakeholder privacy. Digital Parks Africa’ Privacy Policy incorporates relevant legislation as a guideline for sensitive or personal:

- Data Collection;
- Data Retention and Security;
- Data Usage and Disclosure;
- Data Accessibility;
- Data Correction; and
- Data Breach procedures.

2.2 Information Collected by Digital Parks Africa

Digital Parks Africa generally collects some or all the following sensitive/personal information about individual stakeholders when they gain employment or provide information for business purposes:

- Name including any use of a pseudonym;
- Address, phone details and email contact details;
- Employment history;
- Bank account details;
- National identifiers;
- Referee opinions;
- Interview opinions; and
- Any other information that is supplied on documentation or in communications with an Digital Parks Africa representative.

2.3 How Digital Parks Africa Obtains Data

Digital Parks Africa obtains most personal information directly from an individual stakeholder, for purposes which may include (but not be limited to):

- employee management, include the screening of curriculum vitae;
- individuals utilizing the Digital Parks Africa website2; and

- business purposes, including communication by phone, fax, email, in person or other method of communication.

Digital Parks Africa may also, with consent from the data subject, collect personal information from third parties including:

- reference checks with referees; and
- through networking with peers.

2.4 The Purpose of Collection

Digital Parks Africa collects sensitive and personal information about stakeholders to carry out its business functions and fulfil its obligations. These may include (but are not limited to):

- the pursuit of legitimate business objectives;
- complying with government legislation (e.g.: Digital Parks Africa collects tax file numbers to comply with taxation requirements);
- meeting employment obligations to contractors and employees, which may include the processing of sensitive information (e.g.: sick leave).

In addition, Digital Parks Africa may occasionally be required by law to collect, use, and disclose personal information, for example to comply with the requirements of government departments for business data, or in support of a criminal investigation.

2.5 Collection, Use and Disclosure of Sensitive/Personal Information

Digital Parks Africa may only collect, store, process or disclose personal data / information pertaining to an individual:

- if it is lawful to do so;
- by individuals authorized to do so in the course of their duties;
- with the knowledge of the data owner of the personal data / information, unless
- directed otherwise by legal authority; or
- either
    - with the express or implied consent of
        - the data owner;
        - guardian of the data owner of the personal data / information, or;
        - individual legally authorized to act on behalf of the data / information owner; or
    - to satisfy a legitimate commercial purpose; or
    - if required to do so meet a legislative or regulatory obligation.

Sensitive and Personal information may be disclosed to:

- staff of Digital Parks Africa responsible for administering the processes described above;
- health service providers in the event of the administering of emergency health services;
- related bodies and third parties for the administration and provision of selected benefits and services (e.g.: training or policy administration); and
- statutory authorities that may require sensitive data as per legislative requirements.

Digital Parks Africa may collect only the personal data / information that is required to effect the processing requirement.

2.6 Access, Correct or update Personal information

Digital Parks Africa must make reasonable attempts to ensure the accuracy of the personal data / information provided.

To the extent authorized by privacy legislation, Digital Parks Africa must provide data subject access to review and amend sensitive/personal information held by Digital Parks Africa. This may be for a reasonable administration fee, via existing communication channels.

2.7 Security of Sensitive and Personal information

Digital Parks Africa must take all reasonable steps to ensure that sensitive and personal information is held in a secure environment accessed only by authorized persons for approved business purposes.

However, no data processing can be guaranteed to be 100% secure. While Digital Parks Africa strives to protect all sensitive and personal information from misuse, loss, and unauthorized access, Digital Parks Africa cannot guarantee the security of any information transmitted to and from a data source or recipient. Once a transmission is received, Digital Parks Africa will make the best effort to ensure its security in line with Digital Parks Africa data handling procedures.

2.8 Notifiable Data Breaches

Digital Parks Africa recognizes the legislative requirements of the reporting of any breaches of personal or sensitive data / information.

As part of storing sensitive data / information, Digital Parks Africa accommodates data security within its ICT framework.

Digital Parks Africa will use its resources to the best of its capabilities to prevent any personal / sensitive information stored in its database being passed to unsolicited third parties. Unfortunately, Digital Parks Africa cannot provide a 100% guarantee that personal / sensitive information stored will not be obtained by unsolicited third parties.

In cases where Digital Parks Africa has evidence that personal / sensitive information has been obtained by unsolicited parties, Digital Parks Africa will:

- identify the cause of the breach;
- limit any further effects of any breach;
- remedy the breach;

- inform affected individuals;
- report any breaches to any relevant statutory authorities as required; and
- ensure Digital Parks Africa enacts any further processes depending on the nature of the breach.

2.9 Education and Awareness

Digital Parks Africa will incorporate the Privacy Policy into its induction pack, provide privacy training to staff dealing with personal data / information, and communicate privacy principles to all staff using awareness programs.

2.10 Privacy Inquiries

Data Subjects may contact the Information Officer and/or the deputy information officer if they wish to:

- request access to, find out more about or seek amendment of personal data / information held by Digital Parks Africa;
- inquire generally about privacy rights and obligations;
- provide suggestions or feedback in respect of Digital Parks Africa' handling of personal information; or
- make a complaint in relation to Digital Parks Africa handling of personal information.

3. Responsibilities and Accountability

Below are high level functional Responsibilities of the Roles.

The Responsible Person for this Policy is the Chief Executive Officer. Digital Parks Africa reserves the right to monitor and audit networks and systems on a periodic basis, to ensure compliance with this policy.

3.1 The CEO

- The Board is responsible for ensuring that Digital Parks Africa meets its legal, fiduciary, and business obligations to demonstrate compliance with privacy related legislation and other related privacy practices.
- The Board should provide the executive sponsorship of local and global privacy programs.

3.2 System Controller

- Acts in accordance with the Regulation of Interception of Communications and Provision of Communication-Related Information Act, 70 of 2002 (RICA)
- Establishes internal processes for the requesting of monitoring of indirect communications and ensures that key stakeholders utilize them.

- Validates the legitimacy of requests to perform monitoring to protect the right to privacy of the data subject, and to ensure Digital Parks Africa remains compliant with the law.
- Authorizes or declines the monitoring request.
- Where the requests are authorized, set limitations on the extent and duration of the monitoring as appropriate.
- Perform assessments on occasion to ensure that monitoring limitations are adhered to.
- Keep records of all monitoring requests and their outcome.
- Liaise with Digital Parks Africa Legal function as requested when evidence of monitoring approval is required for investigatory purposes.
- Liaise with authorities as required to provide evidence of the legality of monitoring operations.

3.3 Information Officer

- Establish the Privacy Office, albeit virtual
- Liaise with external legal advisor(s) as required
- Define how to integrate “Privacy by Design” into system and product development
- Maintain a data privacy incident/breach response plan
- Maintain a breach notification protocol to affected data subjects
- Maintain a breach reporting protocol to regulators, credit agencies, law enforcement
- Identify ongoing privacy compliance requirements e.g., law, case law, codes, etc.
- Track and address data protection issues identified through Privacy Impact Assessments (PIAs)
- Integrate Data Privacy into Business Risk Assessments
- Maintain an inventory of personal data collected, retained and processed by Digital Parks Africa.
- Conduct due diligence around data privacy and security, including third party service providers and contractors, as well as potential vendors / processors / acquisitions
- Training Digital Parks Africa employees on the relevant privacy/ compliance requirements
- Promote awareness of this Policy
- Identify and evaluate the company’s data processing activities
- To perform data protection impact assessments
- Raise awareness and provide staff training for any employees involved with processing activities.
- Provide a repository of privacy information/monitoring requests

3.4 Employees

- Exercise good judgement regarding the appropriate use of Digital Parks Africa resources in accordance with Digital Parks Africa policies, procedures, standards, and guidelines.
- Digital Parks Africa information assets and information must not be used for any unlawful or prohibited purposes.

- Any Digital Parks Africa data created by an Employee on a Digital Parks Africa system remains the property of Digital Parks Africa.
- Digital Parks Africa employees must take responsibility to familiarize themselves with and adhere to the requirements of this Policy.
- Any Digital Parks Africa employee that processes Personal Information must always ensure and maintain the privacy of the Personal Information processed.
- Digital Parks Africa employees must notify the CEO and the Information officer in the event that a breach is identified.

3.5 Cookie policy

- Digital Parks Africa use cookies. A cookie is a small piece of information stored on your computer or smart phone by the web browser. The two types of cookies used on the Website are described below:
- "Session cookies": These are used to maintain a so-called 'session state' and only lasts for the duration of your use of the Website. A session cookie expires when you close your browser, or if you have not visited the server for a certain period of time. Session cookies are required for the Platform to function optimally, but are not used in any way to identify you personally.

  "Permanent cookies": These cookies permanently store a unique code on your computer or smart device hard drive in order to identify you as an individual user. No Personal Information is stored in permanent cookies. You can view permanent cookies by looking in the cookies directory of your browser installation. These permanent cookies are not required for the website to work, but may enhance your browsing experience.