DIGITAL ECOSYSTEMS (PTY) LTD

(REGISTRATION NUMBER: 2018/100410/07)

PAIA MANUAL

PUBLISHED FOR DIGITAL ECOSYSTEMS (PTY) LTD AS A PRIVATE BODY IN TERMS OF SECTION 51 OF THE PROMOTION OF ACCESS TO INFORMATION ACT 2 OF 2000

TABLE OF CONTENTS

1 INTRODUCTION 1

1.1 AVAILABILITY AND PURPOSE OF THIS PAIA MANUAL 1

1.2 AVAILABILITY OF GUIDES TO THE PAIA AND POPI ACTS 2

2 CONTACT DETAILS 2

3 COMPANY RECORDS 9

3.1 AVAILABILITY OF THE COMPANY'S RECORDS 9

3.2 ACCESS TO HEALTH OR OTHER RECORDS 14

3.3 GROUNDS FOR REFUSAL OF ACCESS TO THE COMPANY'S RECORD 15

4 PROCESSING OF PERSONAL INFORMATION 18

4.1 THE PURPOSES FOR WHICH THE COMPANY PROCESSES PERSONAL INFORMATION 18

4.2 CATEGORIES OF DATA SUBJECTS AND PERSONAL INFORMATION PROCESSED BY THE COMPANY 20

4.3 THE PROCESSING OF PERSONAL INFORMATION AND CATEGORIES OF RECIPIENTS WITH WHOM PERSONAL INFORMATION IS SHARED 20

4.4 INFORMATION SECURITY MEASURES TO PROTECT PERSONAL INFORMATION 21

4.5 TRANS-BORDER FLOWS OF PERSONAL INFORMATION 21

4.6 PERSONAL INFORMATION RECEIVED FROM THIRD PARTIES 22

4.7 DATA SUBJECT REQUESTS (POPIA SECTION 23 - 24) 22

5 PRESCRIBED REQUEST FORMS AND FEES 22

5.1 HOW TO GAIN ACCESS TO RECORDS HELD BY THE COMPANY 22

5.2 PRESCRIBED FEES 23

5.3 ACCESS TO PRESCRIBED FORMS AND FEES 23

6 REMEDIES & DECISION 24

6.1 REMEDIES 24

6.2 TIME AFFORDED TO THE COMPANY 24

ANNEXURE A | FORM 1 25

ANNEXURE B | FORM 2 26

ANNEXURE C | FORM 3 30

1 INTRODUCTION

Digital Ecosystems (Pty) Ltd (the "**Company**") is an investment company operating in the business-to-business technology sector.

This manual is published in terms of Section 51 of the Promotion of Access to Information Act 2 of 2000 ("**PAIA** ") [the "**Manual**"] and provides an outline of the type of records and personal information which the Company holds and processes. The Manual also explains how to submit requests for access to these records in terms of the PAIA. In addition to explaining how to access, or object to personal information held by the Company, or request correction of the personal information, in terms of Sections' 23 and 24 of the Protection of Personal Information Act 4 of 2013 (the "**POPI Act**"), the Manual also explains how to submit requests for access to these records in terms of the PAIA .

The objective of the PAIA is to give effect to the constitutional right to access to information, which information is held by a public or private body, and which information is required for the exercise or protection of any rights. The PAIA recognises the right entrenched in Section 32 of the Constitution of the Republic of South Africa, 1996 and aims to foster a culture of transparency and accountability in public and private bodies by giving effect to the right of access to information.

Accordingly, this PAIA Manual aims to establish and foster a culture of compliance with prevailing data protection legislation, which in turn gives rise to an environment within which the rights to access to information are actively protected and promoted.

Section 9 of the PAIA dictates that the right to access to information is not an unlimited right and is subject to certain limitations, which include limitations which balance the rights which data subjects have to access information against other rights which data subjects and interested parties have, whether it be in terms of the Constitution of the Republic of South Africa, 1996 or otherwise. Some of these rights which the right to access to information are weighed up against are aimed at protecting the fundamental right to privacy and maintaining the confidentiality (whether it be commercial or individual confidentiality) of interested parties so as to maintain acceptable levels of governance.

1.1 Availability and Purpose of this PAIA Manual

This PAIA Manual is published on the Company's website. A copy can also be requested from the Information Officer, which copy may be inspected during normal business hours at the Company's physical address set out in Clause 2 below.

The primary purpose of this PAIA Manual is to facilitate requests for access to information held by the Company, which requests shall be made in accordance with the prescribed procedures and at the rates provided for in Clause 5 of this PAIA Manual. In addition to the above, the further purposes of this PAIA Manual, are to describe the records held by the Company and to clearly articulate the grounds upon which access to any such records may be refused.

1.2 Availability of guides to the PAIA and POPI Acts

The Information Regulator publishes a Guide on how to use PAIA (available in all official languages). Any person may request a copy from the Regulator or our Information Officer using PAIA Form 1.

Guides and forms to the PAIA and POPI Acts can be obtained and queries directed to:

The office of the Information Regulator:	
Physical Address:	Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, Gauteng
Postal Address:	PO Box 31533, Braamfontein Johannesburg, 2017
Phone no.	+27 10 023 5200
Work no.	+27 10 023 5207
E-mail:	enquiries@inforegulator.org.za
Website:	https://inforegulator.org.za/

Note: A Braille version of the PAIA Guide may be obtained directly from the Information Regulator upon request. Requests for Braille or other accessible formats may be submitted to the Information Regulator at the details mentioned above.

2 CONTACT DETAILS

Contact details in terms of Section 51 of the PAIA:

Information Officer	
Name:	Johan Visser (registered with the Regulator via the eServices portal)
Telephone:	011 100 3800
E-mail:	johan@digitalecosystems.co.za
Physical address:	25 Commerce Crescent, Krammerville, 2194
Postal address:	Postnet Suite 41, Private Bag X9, Benmore, Gauteng, 2010

Deputy Information Officer	
Name:	Naomi van Reizig (registered with the Regulator via the eServices portal)
Telephone:	+27 21 418 4004
E-mail:	naomi@digitalecosystems.co.za
Physical address:	25 Commerce Crescent, Krammerville, 2194
Postal address:	Postnet Suite 41, Private Bag X9, Benmore, Gauteng, 2010

General Information

Name of private body:	Digital Ecosystems (Pty) Ltd
Industry:	Technology
Registration number:	2018/100410/07
VAT registration number:	4540303098
Postal address:	POSTNET Suite 41, Private Bag X9,Benmore, Gauteng, 2010
Physical address / Place of business:	25 Commerce Crescent, Krammerville, 2194
Telephone:	011 100 3800
E-mail address:	info@dninvest.co.za
Website:	www.digitalecosystems.co.za

Applicable Legislation:

The Company complies with the following legislation, among others, which may become applicable from time to time, including any subsequent amendments. This compliance is observed in the course of its day-to-day operations.

The table below outlines the categories and subcategories of records processed by the Company. Each category and subcategory may be subject to one or more grounds for refusal of access, as provided for in Chapter 4 of the PAIA. These grounds for refusal are also described in the table under Clause 3.3 below.

	Legislative Reference:	**Records:**
1	**The Basic Conditions of Employment Act No. 75 of 1997**	• Employee details • Labour relations reports. • Information regarding dismissals. • Information on disability, race, and religion. • Employee next of kin or emergency contact details. • Conflict-of-interest declarations. • Education information. • Health and safety records. • Pension fund records. • Leave records. • Internal evaluations and performance records. • Disciplinary records. • Training records. • Background checks.
2	**The Broad-Based Black Economic Empowerment Act No. 53 of 2003 (BBBEE Act)**	• BBBEE status • BBBEE status of suppliers. • Where relevant, supplier / service provider employee information. • Contractor and supplier agreements. • List of suppliers, products, services, and distributors.
3	**The Companies Act No. 71 of 2008**	• MOI; • Minutes of meetings; and • Other records and correspondence.
4	**Compensation for Occupational Injuries and Diseases Act No. 130 of 1993**	• Record of the earnings and other prescribed particulars of all employees.
5	**The Customs and Excise Act 91 of 1964**	• Import and Export Documentation • Excise and Duty Records

		• Licensing and Registration • Inventory and Product Records • Correspondence with SARS Customs Division • Financial and Accounting Records

6	**The Electronic Communications and Transactions Act No. 25 of 2002**	• Electronic Communications
		  ○ Records of data messages (e.g. emails, system notifications)
		  ○ Logs of dispatch and receipt of electronic communications
		  ○ Acknowledgements of receipt of data messages
		• Electronic Transactions
		  ○ Contracts and agreements concluded electronically.
		  ○ Records of automated transactions
		  ○ Electronic signatures and authentication records
		• Information Security and Integrity
		  ○ Records ensuring integrity and accessibility of electronic documents.
		  ○ Backup logs and audit trails
		  ○ Where relevant, encryption and/or authentication protocols
		• Personal Information and Privacy
		  ○ Records of personal data collected electronically.
		  ○ Consent records and privacy notices.
		• E-Government Interactions
		  ○ Electronic filings with government entities
		  ○ Records of compliance with e-government service requirements

7	**The Employment Equity Act No. 55 of 1998**	• Demographic and Designated Group Data
		  ○ Records of race, gender, disability status, and occupational levels of employees
		  ○ Records of designated groups (Black people, women, and people with disabilities)
		• Training and Development Records
		  ○ Records of training provided to designated groups.

		○ Skills development initiatives linked to employment equity. • Declarations ○ EEA declarations
8	**The Income Tax Act No. 58 of 1962**	• Tax Registration and Compliance ○ Income Tax Registration Documents ○ Tax Clearance Certificates ○ VAT Registration and Compliance Records • Employee Tax Records ○ PAYE (Pay-As-You-Earn) Records ○ IRP5 Certificates ○ UIF and SDL Contributions ○ Employee Tax Directives • Company Financial Records ○ Annual Financial Statements ○ Income Tax Returns (ITR14) ○ Supporting Schedules and Calculations ○ Provisional Tax Returns • Transactional Records ○ Invoices and Receipts ○ Bank Statements ○ Expense Records ○ Asset Registers • Third-Party Tax Records ○ Records of payments to contractors (e.g. IT3 certificates) ○ Withholding tax documentation • Correspondence with SARS ○ Notices of Assessment ○ Objections and Appeals ○ Audit and Verification Correspondence • Retirement and Benefit Records ○ Pension Fund Contributions ○ Medical Aid Contributions (for tax deduction purposes) • Donations and Deductions ○ Records of Donations (e.g. Section 18A certificates) ○ Other deductible expenses and supporting documentation
9	**The Labour Relations Act No. 66 of 1995**	• Employee Relations Records ○ Disciplinary Records ○ Grievance Records

		○ Records of Dispute Resolution Processes (e.g. CCMA referrals) ○ Records of Incapacity Hearings • Employment Contracts & Conditions ○ Employment Contracts ○ Amendments to Terms and Conditions ○ Retrenchment Documentation • Dismissal and Termination Records ○ Records of Dismissals ○ Exit Interviews ○ Settlement Agreements • Correspondence and Legal Proceedings ○ Correspondence with Employees ○ Legal Opinions and Case Files • Litigation Records
10	**The Occupational Health and Safety Act No. 4 of 2013 (OHSA)**	• Policies and Management Framework ○ Health and safety policy documents adopted by the Company. ○ Risk assessment reports for workplaces, processes, and tasks. • Incident, Accident, and Injury Records ○ Accident and incident register, detailing all workplace injuries, dangerous occurrences, and/or occupational diseases. ○ Individual accident report forms and investigation findings ○ Notices of injury or occupational disease submitted to the Department of Labour (Form 6) and proof of submission. • Appointments, Committees and Training ○ Written appointments of health and safety representatives and members of the health and safety committee Section 17 of OHSA ○ Minutes and attendance registers of health and safety committee meetings ○ Records of mandatory safety training sessions, including induction, refresher courses, and specialist training certificates • Correspondence and Reports

		○ Correspondence with and reports from external safety bodies and approved inspection authorities • Displayed Information and Internal Communications ○ Proof of display of the OHSA, regulations and approved codes of practice at conspicuous locations Section 19 of OHSA ○ Safety bulletins, newsletters, or circulars issued to employees regarding OHSA compliance
11	**The Promotion of Access to Information Act No. 2 of 2000 (PAIA)**	• Governance and Policy Documents ○ PAIA Manual ○ Appointment letters of the Information Officer and Deputy Information Officer • Request Handling and Access Records • Training and Awareness Materials • Regulatory Compliance and Reporting ○ Annual returns and compliance reports submitted to the Information Regulator Section 32 of PAIA • Communication and Publication Records
12	**The Protection of Personal Information Act (POPIA)**	• Governance and Policy Documents ○ Data protection policy and procedural guidelines ○ Appointment letters of the Information Officer and Deputy Information Officer ○ Privacy governance framework • Request Handling and Access Records • Training and Awareness Records • Regulatory Compliance and Reporting ○ Records of processing operations and processing activity ○ Data Protection Impact Assessments ○ Data breach incident reports and breach-notification logs ○ Copies of breach notifications sent to the Information Regulator and affected data subjects. ○ IT audit reports • Communication and Publication Records

		○ Privacy notices and policy statements for employees, clients, and third parties
13	**Promotion of Equality and Prevention of Unfair Discrimination Act No. 4 of 2000**	• Governance and Policy Documents ○ Equality policies and procedures • Complaint Handling and Resolution Records • Training and Awareness Materials • Workforce demographic statistics and employment equity data
14	**Regulation of Interception of Communications and Provision of Communication-Related Information Act No. 70 of 2002**	• Governance and Policy Documents • Security and Incident Records
15	**The Skills Development Act No. 97 of 1998**	• Governance and Policy Documents • Learnership and Skills Programme Records • Sector Education and Training Authority (SETA) Records • Training and Development Records • Employment Services Records
16	**The Skills Development Levies Act No. 9 of 1999**	• Governance and Policy Documents • Financial and Levy Payment Records • Regulatory Compliance and Reporting Records • Employment and Payroll Records
17	**The Unemployment Insurance Act No. 63 of 2001**	• Governance and Policy Documents • Employee and Contributor Records • UIF Contribution and Payment Records • Claim and Benefit Records • Regulatory Compliance and Reporting Records

3 COMPANY RECORDS

3.1 Availability of the Company's Records

The provisions of the PAIA, specifically the provisions of Section 50 of the Act, dictate that a requester for access to information must be afforded access to any record of the Company if the following requirements are met:

- where a particular record is required for the exercise or protection of any rights (Section 50(1)(a) of PAIA);

- where a requester complies with the procedural requirements set forth in the PAIA relating to a request for access to particular records (Section 50(1)(b) of PAIA); and

- where access to that particular record is not refused in terms of any of the grounds for refusal to access contemplated in terms of Chapter 4 of the PAIA (Section 50(1)(c) of PAIA).

The below table sets forth the categories and subcategories of records which the Company processes. Each category and subcategory of records set out below may be subject to anyone (or a number) of the grounds upon which the Company may refuse access to records. These grounds for refusal are set out in Chapter 4 of the PAIA, as well as described in the table at Clause 3.3 below.

Data Subject Categories	**Personal information that may be processed**
Personnel (including directors, executive directors, non-executive directors, permanent, temporary, part-time staff, and contract workers)	• **Basic Identifiers** o Name, Surname, Identity Number, Date of Birth, Place of Birth, Gender, Marital Status, Nationality • **Contact Information** o Address (including proof of address), Email Address, Telephone Number • **Employment Information** o Employer, Job Title, Conditions of Employment, Contracts and Agreements, Personnel Files, Statutory Employee Records, Retirement Fund Records, Employee Payments and Benefits (statutory and contractual), Employee Leave Records, Budget Projections in Respect of Staff • **Performance & Conduct** o Internal Evaluation Records, Performance Management Records,

	Disciplinary Records, Records of Disciplinary Hearings and Findings, Records of Incapacity Proceedings • **Training & Development** o Training Schedules and Materials • **Third-Party Records** o Records provided by third parties about employees (e.g. references, background checks) • **Background Checks** o Qualification Checks, Credit Checks, Criminal Record Checks • **Health & Safety** o Medical Aid Records, Medical Information (related to incapacity proceedings), Records of Occupational Injuries and Diseases • **Compliance & Legal** o Employee Declarations in Terms of the Employment Equity Act (EEA), Employee-Related Contractual and Quasi-Legal Records • **Organisational Information** o Organisational Structure, Employment Policies and Procedures • **Correspondence** o Internal Records and Correspondence, Correspondence with or About Employees
Client / Customer-Related Records Please motivate any request for client / customer information	• Any records a client / customer has provided to the Company or a third party acting for or on behalf of the Company.

very carefully, having regard to Sections 63 to 67 of the PAIA.	• Contractual information • Client / customer needs assessments • Personal records of clients / customers • Credit information and other research conducted in respect of clients / customers. • Any records a third party has provided to the Company about clients / customers. • Confidential, privileged, contractual, and quasi legal records of clients / customers • Client / customer evaluation/review records • Client / customer profiling • Performance research conducted on behalf of clients / customers or about clients / customers. • Any records a third party has provided to the Company either directly or indirectly. • Records generated by or within the Company pertaining to clients / customers, including transactional records
Technical Records	• Technical reports • Technical data • Plans, brands, and trademarks forming part of the intellectual property rights of the Company.
Third-Party	**Records Held by Third Parties About the Company, Employees, or Clients**: • Personnel, Client/Customer, or Company Records held by third parties. • Records provided by third parties about contractors, suppliers, or clients/customers. • Employee, Client, or Company Records held externally (e.g.,

	payroll service providers, outsourced HR, or IT systems) **Records Held by the Company Pertaining to Third Parties** • VAT Numbers, Banking Details, Names • Financial Records • Correspondence • Contractual Records • Electronic Mail, Logs • Records provided by third parties • Service Level Agreements (SLAs) • Contact Details of Suppliers • Details of Customers/Clients (e.g., contact details, transaction history) • Licenses and General Conditions for Conducting Business • Agreements with Stakeholders
Other Records	• Information relating to the Company's own business activities
Internal Records	• Basic Identifiers o Name, Surname, Address (including proof of address), Email Address, Telephone Number, Gender, Marital Status, Date and Place of Birth, Nationality • Professional Information o Employer, Job Title, Registration Number • Governance & Statutory Records o Records relating to incorporation, Statutory Records, Minutes of Meetings (including Executive Committee and subcommittees), Resolutions and Directives

	• Financial Records
	  ○ Financial Records, Company Pension Fund Records and Rules, Insurance Records (e.g. professional indemnity, group life assurance, disability income protection)
	• Operational Records
	• Intellectual Property Records
	• Marketing Records
	• BBBEE Information
	• Internal Documentation
	  ○ Internal Correspondence, Internal Investigation Reports, Policies, Procedures, and Codes
	• Information Technology
	  ○ IT Records including Computer Software, Support and Maintenance Agreements

In terms of Section 52 of the PAIA, the Company makes some records automatically available, without the need to request access to them:

Type of record	**How you can access it**
Memorandum of incorporation (MOI)	The Companies and Intellectual Property Commission
Directors' names	BizPortal
Documents of incorporation	The Companies and Intellectual Property Commission
Banking details	By e-mail
Company Overview and Public Disclosures	www.digitalecosystems.co.za

No additional categories have been submitted to the Information Regulator for automatic availability in terms of Section 52(2) of PAIA. Only the categories listed above are automatically available and shall be updated as required.

3.2 Access to Health or Other Records

If a request for access to health or other records provided by a health practitioner, in

their capacity as such, relates to the physical, mental health, or well-being of the requester, or if the request has been made on behalf of the person to whom the record relates ("**the relevant person**"), and the Company's Information Officer is of the opinion that the disclosure of the record to the relevant person might cause harm to his or her physical, mental health or well-being, the Company's Information Officer may, before giving access to such record consult with a health practitioner who has been nominated by the relevant person.

If the relevant person is below the age of 16 years, a person having parental responsibilities for the relevant person must make the above nomination and if the relevant person is incapable of managing his or her affairs, a person appointed by the court to manage those affairs must make that nomination.

If, after being given access to the relevant record, the health practitioner consulted is of the opinion that the disclosure of the record to the relevant person, would be likely to cause serious harm to his or her physical, mental health or well-being, the Information Officer may only grant access to the relevant record if the requester proves that adequate provision is made for such counselling or arrangements as are reasonably practicable before, during or after the disclosure of the record to limit, alleviate or avoid such harm to the relevant person. Before access to the record is given to a requester, the person responsible for such counselling or arrangement must be given access to the record.

3.3 Grounds for Refusal of Access to the Company's Record

Upon receipt of a request for access to information, the Company will be required to consider such a request in light of the provisions of Section 50 of the PAIA. Subject to such consideration, the Company will be required to either grant such a request or refuse such a request. If the Company elects to refuse access to a particular record, such refusal will be subject to the Company's interpretation of the various prescribed grounds for refusal as set forth in Chapter 4 of the PAIA and in the table below:

Ground(s) For Refusal	**Description and Explanation of Ground(s) for Refusal**
Mandatory protection of privacy of third party who is a natural person [Section 63 of PAIA]	The Company may refuse access to a record if the disclosure of that record would involve the unreasonable disclosure of personal information relating to a third party, including a deceased individual.

Mandatory protection of commercial information of third party [Section 64 of PAIA]	The Company may refuse a request for access to a record if the record comprises of or is constituted by the following information relating to a third party – • Trade secrets of a third party. • Financial, commercial, scientific, or technical information, other than trade secrets, of a third party, which if disclosed is likely to cause harm to the commercial or financial interests of the third party. • Information which has been supplied in confidence by a third party, the disclosure of which could reasonably be expected to place the third party at a disadvantage in contractual or other negotiations or is likely to prejudice the third party in commercial competition.
Mandatory protection of certain confidential information of a third party [Section 65 of PAIA]	The Company may refuse access to a record which if disclosed would constitute an action for breach of a duty of confidence owed to a third party in terms of an agreement or contractual. relationship.
Mandatory protection of safety of individuals and protection of property [Section 66 of PAIA]	The Company may refuse a request for access to a record if its disclosure could reasonably be expected to endanger the life or physical safety of an individual, or if its disclosure would be likely to prejudice or impair the security of: • a building, structure, or system, including but not limited to a computer or communication system, a means of transport or any other property. • method(s), system(s), plans or procedures for the protection of an individual in accordance with a witness protection scheme, the safety of the public, or any part of the public or the security of property.

Commercial information of Private Body [Section 68 of PAIA]	The Company may refuse a request for access to a record if the record contains (or comprises of): • Trade secrets of the Private Body. • Financial, commercial, scientific, or technical information, other than trade secrets of the Private Body, the disclosure of which would be likely to cause harm to the commercial or financial interests of the Private Body. • Information, the disclosure of which could reasonably be expected to put the Private Body at a disadvantage in contractual or other negotiations or prejudice the Private Body in commercial competition. • A computer programme (as defined in Section 1(1) of the Copyright Act 98 of 1978 as amended) owned by the Private Body, except insofar as it is required to give access to a record to which access is granted in terms of the PAIA. Act.
Mandatory protection of research information of third party, and protection of research information of private body [Section 69 of PAIA]	The Company may refuse a request for access to a record if the record contains information about research being or to be carried out by or on behalf of a third party/private body, the disclosure of which would be likely to expose the third party/private body, a person that is (or will be) carrying out the research on behalf of the third party/private body, or the subject matter of the research to serious disadvantage.

4 PROCESSING OF PERSONAL INFORMATION

Data Subject Information at Collection (Section 18 of the POPI Act)

The Company takes any activities relating to the protection and processing of personal information (as defined in terms of the provisions of Section 1 of the POPI Act) very seriously. To promote the constitutional right to privacy, as well as to play its part in promoting the rights protected in terms of the POPI Act, the Company undertakes to, in so far as is required of it, observe the requirements and conditions for the lawful processing of personal information.

When collecting personal information, the Company takes reasonably practicable steps to make data subjects aware of: (a) the information collected and, where not collected directly, the source; (b) our name and address; (c) the purposes of collection; (d) whether the supply is mandatory or voluntary; (e) the consequences of not providing it; (f) any particular law authorising collection; (g) any intended transfers to foreign countries and the protection there; and (h) further information necessary to ensure reasonable processing, such as recipients or categories of recipients, the nature of the information, the rights of access/correction/objection, and the right to complain to the Information Regulator (with contact details).

4.1 The Purposes for which The Company Processes Personal Information

The Company may process personal information for a variety of purposes, which may include, but is not limited to, the following purposes:

- to provide or manage any information, products and/or services requested by or delivered to data subjects in general.
- to establish a data subject's needs, wants and preferences in relation to the products and/or services provided by us and/or any affiliate of the Company.
- to help the Company identify data subjects when they engage with the Company.
- to facilitate the delivery of products and/or services to clients / customers.
- to facilitate registration of the Company's offerings.
- to verify information provided by a data subject.
- to allocate unique identifiers to data subjects for the purpose of securely storing, retaining, and recalling their personal information/personal data from time to time.

- to maintain records of data subjects (including client / customer records).
- to maintain third party records.
- for recruitment purposes.
- for employment purposes.
- for general administration purposes.
- for legal and/or contractual purposes.
- for health and safety purposes.
- to monitor access, secure and manage any facilities operated by the Company regardless of location.
- to transact with data subjects;
- to improve the quality of the Company's services;
- to transfer personal information/personal data to third party service providers to enable the Company to deliver services to its clients / customers and/or participants in its various offerings;
- to transfer personal information/personal data to any affiliate of the Company so as to enable the relevant affiliate of the Company to market its products and/or services to data subjects;
- to analyse the personal information / personal data collected for research and statistical purposes;
- to help recover bad debts;
- to transfer personal information/personal data across the borders of South Africa to other jurisdictions if it is required;
- to identify other products and/or services which might be of interest to the Company's clients / customers and data subjects in general, and to inform them of such products and/or services.
- to identify any products and services offered by any affiliates of the Company which might be of interest to data subjects in general, as well as to inform them of such products and/or services;
- to comply with any laws applicable to the Company and in some instances affiliates of the Company.

4.2 Categories of Data Subjects and Personal Information Processed by the Company

The categories of data subjects may include, but are not limited to, the following:

- Employees, sales personnel, client's / customer's staff and/or clients, any persons who deal with the company;
- any affiliate of the Company;
- service providers;
- independent contractors;
- agents;
- consultants;
- users of the Company's platforms; and
- users of the Company's website or any other digital application interface.

The categories of personal information processed by the Company may include, but are not limited to, the following –

- full names (name and surname);
- identity or passport numbers;
- e-mail, physical and postal addresses;
- telephone numbers;
- information relating to the data subject's occupation;
- gender;
- date of birth;
- registration numbers;
- financial information, including banking account information;
- statutory information;
- geo-location information;
- unique identifiers; and
- personal information submitted that forms part of onboarding/registration/employment documentation from time to time.

4.3 The Processing of Personal Information and Categories of Recipients with Whom Personal Information Is Shared

Subject to any relevant terms and conditions of use which may be applicable when a data subject engages with the Company, we may share the personal information of any data subject we process for any of the purposes outlined in Clause 4.1 mentioned above , with the following third parties, whether such third parties qualify as "**Responsible Parties**" in terms of Section 1 of the POPI Act or not:

- any affiliate of the Company from time to time;
- any relevant service providers and suppliers;
- any relevant regulatory authorities who may govern the Company in undertaking its operations;
- any approved service provider, contractor, or supplier with whom the Company has an agreement;
- any approved business partners who provide products and services to the Company; and

- any approved service providers or authorised agents who perform services on the Company's behalf.

The Company processes personal information to facilitate and enhance the delivery of products and services to its clients / customers, foster a legally compliant workplace environment, as well as safeguard the personal information relating to any data subjects which it in fact holds. We undertake to process any personal information in a manner which promotes the constitutional right to privacy, retains accountability and data subject participation. In any circumstances where we process the personal information of data subjects, the Company maintains appropriate privacy notices where the purposes of the processing of any personal information and the processing takes place, is recorded and communicated to data subjects.

We conclude operator agreements with all processors in terms of Sections 20 to 21 of POPI Act and retain oversight of security, confidentiality, and sub-processing.

4.4 Information Security Measures to Protect Personal Information

We have, and continue to, implement reasonable, technical, and organisational measures for the protection of personal information processed by the Company. We at all times take reasonable and appropriate security measures to secure the integrity and confidentiality of personal information in our possession in order to guard against:

- the loss of, damage to or unauthorised destruction of personal information;
- the unlawful access or processing of personal information; or
- the wilful manipulation of personal information.

We will take steps to ensure that any third-party process operators (as defined in terms of Section 1 of the POPI Act) who process personal information on behalf of the Company apply adequate safeguards as outlined above.

In the event of a security compromise, we will notify the Information Regulator and affected data subjects as soon as reasonably possible, using the Regulator's required notification template (SCN1), with the content specified in the Guidelines.

4.5 Trans-Border Flows of Personal Information

We transfer personal information cross-border only if one of Section 72 of the POPI Act safeguards applies: (i) the recipient is subject to a **law**, **binding corporate rules** or a **binding agreement** that provides an adequate level of protection (including onward-transfer limits); (ii) the **data subject consents**; (iii) the transfer is **necessary for a contract** with, or in the interest of, the data subject; or (iv) the transfer benefits the data subject where consent can't practicably be obtained but would likely be given. We assess recipient protections and seek to keep records of

reliance.

4.6 Personal Information Received from Third Parties

When the Company receives personal information from any third party on behalf of a data subject, we require confirmation that such a third party has written consent from the data subject indicating that said data subject is aware of the contents of this PAIA Manual and the Company's Privacy Policy, and do not have any objection to our processing their personal information accordingly.

4.7 Data Subject Requests Sections 23 - 24 POPI Act

On adequate proof of identity, data subjects can request confirmation of whether we hold their personal information and access to a record/description thereof (including recipients), within a reasonable time and in an understandable form (fees may apply). They may also request correction or deletion where information is inaccurate or no longer authorised to be retained. Requests can be made using POPI Act Form 1 and Form 2 on the Regulator's site or via our Information Officer as contemplated at Clause 5 below.

5 PRESCRIBED REQUEST FORMS AND FEES

5.1 How To Gain Access to Records Held by the Company

Records which are held by requests may access the Company for such access to information and documentation in the prescribed manner and subject to certain requirements being met. In this regard, a requester is any person making a request for access to a record held by the Company. There are two types of requesters:

- A Personal Requester: A personal requester is a requester who is seeking access to a record containing personal information about the requester. The Company will voluntarily provide the requested information or give access to any record with regard to the requester's personal information. In this regard, the prescribed fees for the reproduction of this information requested may be charged.

- Other Requester: This requester (other than a personal requester) is entitled to request access to information on third parties. The Company is, however, not obliged to voluntarily grant access and the requester must fulfil the procedural requirements for access in terms of the PAIA, including the payment of a request and access fee.

Requests for access to records must be made by completing the prescribed Form 2 (Regulation 7), included as Annexure B to this Manual, and paying the requester's fee. Where such access is granted in terms of this PAIA Manual, the information and documentation will be made available at the offices of the Company (the particulars of which appear in Clause 2 above) or in the manner requested, should this be reasonable and possible. The manner of access will include:

- Perusal with copying of material, if needed, and at the prescribed fee for copies;
- Access to visual, audio-visual material with a transcription, dubbing, copying or both, if required.

To facilitate the processing of any request by a requester for information or documentation in terms of this PAIA Manual, requesters are required to follow the procedure set forth herein below:

i. Use the prescribed Form 2 attached hereto as **Annexure B**.
ii. Address your request to the Information Officer.
iii. Provide sufficient detail to enable the Company or any authorised person dealing with a request to identify:

a) The record(s) requested;
b) The requestor (and, if an agent is lodging the request or behalf of someone, proof of capacity and authorisation);
c) The South African postal address, email address, or fax number of the requestor;
d) The form of access required;
e) If the requester wishes to be informed of the decision in any manner (in addition to being informed in writing), the manner and particulars thereof;
f) The right which the requestor is seeking to exercise or protect with an explanation of the reason the record is required in order to exercise or protect the right.

5.2 Prescribed Fees

The following applies to requests (other than personal requests):

i. A requestor is required to pay the prescribed fees before a request will be processed.
ii. If the preparation of the record requested requires more than the prescribed hours, a deposit shall be paid (calculated on one third of total amount per request).
iii. A requestor may lodge an application with a court against the tender/payment of the request fee and/or deposit.
iv. Records may be withheld until the fees have been paid.

The detailed Fee Structure as prescribed in terms of Section 54 of the PAIA is reflected in the prescribed form 3 attached hereto as **Annexure C.**

5.3 Access to Prescribed Forms and Fees

Prescribed forms and fees are published on the Company's website. Copies can also

be requested from the Information Officer (see contact details in Clause 2).

6 REMEDIES & DECISION

6.1 Remedies

The Company does not have an internal appeal procedure regarding PAIA and POPI Act requests for access to information. As such, the decision made by the Information Officer, is final.

If a request is denied and the requester is dissatisfied with the Information Officer's decision, the requestor will be required to exercise such external remedies at their disposal if a request for information is refused.

In terms of Section 77A of the PAIA, if a request is denied by the head of a private body, the requester may lodge a complaint with the Information Regulator using PAIA **Form 5**, available on the Regulator's website or eServices portal, within **180 days** of the decision.

A requester is further entitled in terms of Section 78(2)(b) of the PAIA to apply to a court with appropriate jurisdiction within 180 days for appropriate relief.

6.2 Time Afforded to the Company

The Company is required to, within 30 (thirty) days of receipt of a request, decide whether to grant or decline the request and, if required, provide the requester with reasons to that effect.

The 30 (thirty) day period stipulated in the Clause above may be extended for a further period of not more than 30 (thirty) days if the request is for a large amount of information, or the request requires an extensive search for information which cannot reasonably be obtained within the originally stipulated 30 (thirty) day period.

In the circumstances contemplated in the Clause above. The Company will notify the requester in writing should an extension be sought.

COMPILED BY DIGITAL ECOSYSTEMS (PTY) LTD

DATE: 25 May 2026

ANNEXURE A | FORM 1

REQUEST FOR A COPY OF THE GUIDE

FORM 1
[Regulation 2]

I,

Full names:				
In my capacity as (mark with "x"):	Information officer		Other	
Name of *public/private body *(if applicable)*				
Postal Address:				
Street Address:				
E-mail Address:				
Facsimile:				
Contact numbers:	Tel.(B):		Cellular:	

hereby request the following copy(ies) of the Guide:

Language *(mark with "X")*	No of copies	Language *(mark with "X")*	No of copies
☐ Sepedi		☐ Sesotho	
☐ Setswana		☐ siSwati	
☐ Tshivenda		☐ Xitsonga	
☐ Afrikaans		☐ English	
☐ isiNdebele		☐ isiXhosa	
☐ isiZulu			

Manner of collection *(mark with "x"):*

Personal collection	Postal address	Facsimile	Electronic communication (Please specify)

Signed at _____this _____day of _____20 _____

_____
Signature of requester

ANNEXURE B | FORM 2

REQUEST FOR ACCESS TO RECORD

[Regulation 7]

NOTE:

1. Proof of identity must be attached by the requester.

2. If requests made on behalf of another person, proof of such authorisation, must be attached to this form.

TO: The Information Officer

Information Officer:	Deputy Information Officer:
Address:	Address:
Email:	Email:
Telephone Number:	Telephone Number:

Mark with an "**X**"

[] Request is made in my own name

[ ] Request is made on behalf of another person

PERSONAL INFORMATION		
Full Names		
Identity Number		
Capacity in which request is made *(when made on behalf of another person)*		
Postal Address		
Street Address		
E-mail Address		
Contact Numbers	Tel:	
	Facsimile:	
	Cellular:	
Full names of person on whose behalf request is made *(if applicable)*		
Identity Number		
Postal Address		

Street Address		
E-mail Address		
Contact Numbers	Tel:	
	Facsimile:	
	Cellular:	

PARTICULARS OF RECORD REQUESTED *Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located. (If the provided space is inadequate, please continue on a separate page and attach it to this form. All additional pages must be signed.)*	
Description of record or relevant part of the record	
Reference number, if available	
Any further particulars of record	

TYPE OF RECORD *(Mark the applicable box with an "X")*	
Record is in written or printed form	
Record comprises virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Record consists of recorded words or information which can be reproduced in sound	
Record is held on a computer or in an electronic, or machine-readable form	

FORM OF ACCESS *(Mark the applicable box with an "X")*	
Printed copy of record (including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)	
Written or printed transcription of virtual images (this includes photographs, slides, video recordings, computer-generated images, sketches, etc)	
Transcription of soundtrack (written or printed document)	

Copy of record on flash drive (including virtual images and soundtracks)	
Copy of record on compact disc drive (including virtual images and soundtracks)	
Copy of record saved on cloud storage server	
MANNER OF ACCESS *(Mark the applicable box with an "**X**")*	
Personal inspection of record at registered address of public/private body (including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)	
Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format (Including transcriptions)	
E-mail of information (including soundtracks if possible)	
Cloud share/file transfer	
Preferred language (Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)	
PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED *If the provided space is inadequate, please continue on a separate page and attach it to this Form. The requester must sign all the additional pages.*	
Indicate which right is to be exercised or protected	
Explain why the record requested is required for the exercise or protection of the aforementioned right:	
FEES	

a) *A request fee must be paid before the request will be considered.* b) *You will be notified of the amount of the access fee to be paid.* c) *The fee payable for access to a record depends on the form in which access is required, and the reasonable time required to search for and prepare a record.* d) *If you qualify for exemption of the payment of any fee, please state the reason for exemption*

Reason	

You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any. Please indicate your preferred manner of correspondence:

Postal Address	**Facsimile**	**Electronic Communication** ***(Please specify)***

Signed at _____ this _____ day of _____ 20___.

_____

Signature of Requester / person on whose behalf request is made.

_____

FOR OFFICIAL USE

Reference number	
Request received by: *(State rank, Name and Surname of Information Officer)*	
Date received	
Access fees	
Deposit (if any)	

_____

Signature of Information Officer

ANNEXURE C | FORM 3
OUTCOME OF REQUEST AND OF FEES PAYABLE
[Regulation 8]

Note:
1. If your request is granted the—
(a) amount of the deposit, (if any), is payable before your request is processed; and
(b) requested record/portion of the record will only be released once proof of full payment is received.
2. Please use the reference number hereunder in all future correspondence.

Reference Number: _____

TO: _____
_____
_____
_____

Your request dated _____refers.

1. **You requested:**

Personal inspection of information at registered address of public/private body (including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form) is free of charge. You are required to make an appointment for the inspection of the information and to bring this Form with you. If you then require any form of reproduction of the information, you will be liable for the fees prescribed in Annexure C.	

OR

2. **You requested:**

Printed copies of the information (including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)	
Written or printed transcription of virtual images (this includes photographs, slides, video recordings, computer-generated images, sketches, etc)	
Transcription of soundtrack (written or printed document)	
Copy of information on flash drive (including virtual images and soundtracks)	
Copy of information on compact disc drive (including virtual images and soundtracks)	
Copy of record saved on cloud storage server	

3. **To be submitted:**

Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format(including transcriptions)	
E-mail of information (including soundtracks if possible)	
Cloud share/file transfer	
Preferred language: (Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)	

Kindly note that your request has been: [] Approved.
[] Denied, for the following reasons:

4. Fees payable with regards to your request:

Item	Cost per A4-size page or part thereof/item	Number of pages/items	Total
Photocopy			
Printed copy			
For a copy in a computer-readable form on: Flash drive To be provided by requestor ii) Compact disc If provided by requestor If provided too the requestor	R40.00 R40.00 R60.00		
For a transcription of visual images per A4-size page	Service to be outsourced. Will depend on the Quotation of		
Copy of visual images			

	The service provider		
Transcription of an audio record, per A4-size	R24.00		
Copy of an audio record: Flash drive To be provided by requestor Compact disc	R40.00		
• If provided by requestor • If provided to the requestor	R40.00 R60.00		
Postage, e-mail, or any other electronic transfer:	Actual Costs		
TOTAL:			

5. **Deposit payable (if search exceeds six hours):**

[] Yes [] No

Hours of search		Amount of deposit *(calculated on one third of total amount per request)*	

The amount must be paid into the following Bank account:

Name of Bank: _____

Name of account holder: _____

Type of account: _____ Account number: _____ Branch Code: _____ Reference Nr: _____

Submit proof of payment to: _____

Signed at _____ this _____ day of _____ 20___.

_____

Signature of Information Officer

ANNEXURE D | PRIVACY POLICY

DIGITAL ECOSYSTEMS PROPRIETARY LIMITED ("COMPANY")

1 DEFINITIONS

In this Policy (as defined below), unless the context requires otherwise, the following capitalised terms shall have the meanings given to them —

1.1 "**Active Processing**" means instances where the Company has directly been provided with the Personal Information/Personal Data of Data Subjects, such as when Data Subjects submit an enquiry in respect of our Services, or when Data Subjects provide Personal Information/Personal Data to the Company pursuant to concluding any commercial agreement(s) with the Company;

1.2 "**Anonymisation**" means the Processing of Personal Information/Personal Data in such a manner that the Personal Information/Personal Data can no longer be attributed to Data Subjects without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Information/Personal Data are not attributed to Data Subjects;

1.3 "**Applicable Laws**" means any laws applicable to Personal Data and Personal Information and includes any statute, regulation, notice, policy, directive, ruling or subordinate legislation; the common law; any binding court order, judgement or ruling; any applicable industry code, policy or standard enforceable by law; or any applicable direction, policy or order that is given by any regulator, competent authority or organ of state or statutory industry body;

1.4 "**Biometrics**" means a technique of personal identification that is based on physical, physiological, or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition;

1.5 "**Child**" means any natural person under the age of 18 years;

1.6 "**Competent Person**" means anyone who is legally competent to consent to any action or decision being taken by any matter concerning a child, for example a parent or legal guardian;

1.7 "**Controller**" means the Company, in circumstances where it Processes Personal Data

(as defined in Article 4 of the GDPR);

1.8 "**Consent**" means any voluntary, specific, and informed expression of will in terms of which permission is given for the Processing of Personal Information;

1.9 "**Cookies**" means small text files that store Non-Personally Identifiable Information/Data about Data Subjects, either temporarily in connection with a Data Subjects Internet Protocol (IP) address (known as a temporary or session cookie, and deleted once a Data Subject closes their browser window) or more permanently on the hard drive of a Data Subject's device (known as a permanent or persistent cookie). The Company Website(s) or Mobile Application(s) may from time-to-time use session cookies so that Data Subject's do not have to fill in the same information from page to page within our website(s) or Mobile Application(s). If Data Subject's elect not to receive cookies, they may be able to view some, but not all, of the content on our website(s) or Mobile Application(s);

1.10 "**Customer(s)**" means any natural person(s), or juristic person(s), who have concluded an agreement with the Company in terms of which such Customer procures the Products or Services provided by the Company;

1.11 "**Data Subject**" means the Company's Customer(s) or any Third Party in respect of whom the Company Processes Personal Information/Personal Data;

1.12 "**Data Processing Infrastructure**" means any and all systems, networks, servers, workstations, laptops, mobile devices, web applications, mobile applications, cloud storages, websites owned, controlled, or operated by the Company;

1.13 "**Embedded Scripts**" means, programming code that is designed to collect information about a Data Subject's interactions with the relevant website(s) or Mobile Application(s). It is temporarily downloaded onto a Data Subject's device from our web server or a Third-Party Operator. This program is active only while a Data Subject is connected to the relevant website(s) or Mobile Application(s) and is deleted or deactivated thereafter;

1.14 "**Electronic Means**" means, in relation to the Processing of any Personal Information/Personal Data, the use of any Website(s), Mobile Application(s), electronic mail (email), text, voice, sound or image messages by the Company;

1.15 "**GDPR**" means the General Data Protection Regulation, which is a European law that

governs all collection and processing of personal data from individuals inside the European Union;

1.16 "**Group Company**" means any company forming part of the group of companies to which the Company is a part or a company or entity affiliated to the Company;

1.17 "**Inactive Processing**" means instances where the Company has not actively been provided with the Personal Information/Personal Data of Data Subjects, such as when the Company deploys Passive Processing Means to collect information from Data Subjects. These Passive Processing Means allow the Company to Process certain kinds of Non-personally Identifiable Information which can perhaps not be linked to Data Subjects;

1.18 "**Mobile Application(s)**" means any multi-device software application, whether in web-based format or device-native format, to which this Privacy Policy relates and through which Customer(s) and Third Parties gain access to the Company's Products and/or Services;

1.19 "**Mobile Device Identifier**" means device information if you access our website(s) or Mobile Application(s) through mobile devices. Certain features of the relevant website(s) or Mobile Application(s) may require collection of mobile phone numbers, and we may associate that phone number with the mobile device identifiers. Additionally, some mobile phone service providers operate systems that pinpoint the physical location of devices that use their service. Depending on the provider, the Company and/or our Third-Party Operators may receive this information. If the Company associates any such passively collected information with the Personal Information/Personal Data of Data Subjects, we will treat the combined information as Personal Information/Personal Data as contemplated in this Policy;

1.20 **"Non-Electronic Means**" means, in relation to the Processing of any Personal Information/Personal Data, the use of traditional means of Processing, such as hard copy documents, traditional filing systems deployed for the storage and retention of Personal Information/Personal Data and face-to-face personal engagements with Data Subjects;

1.21 "**Non-Personally Identifiable Information/Data**" means any information/data which cannot be linked to Data Subjects, such as an internet domain name, the type of

web browser used by a Data Subject, the type of operating system relied on by a Data Subject, the date and time of a Data Subject's visit to our Website(s) and Mobile Application(s), the specific pages a Data Subject may have visited, and the address of the website which a Data Subjects may have visited prior to entering or gaining access to the Company's Website(s) or Mobile Application(s);

1.22 "**Operator**" means a person or entity who Processes Personal Information/Data for a Responsible Party;

1.23 "**Passive Processing Means** " means the use of technologies to facilitate the Inactive Processing of Personal Information/Personal Data, namely the use of Cookies, Web Beacons, Embedded Scripts, and/or Mobile Device Identifiers;

1.24 "**Personal Data**" (as defined in Article 4 of the GDPR) means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, which in the context of the Company shall comprise of the types of Personal Data recorded in this Policy below;

1.25 "**Personal Information**" shall have the same meaning as is given in Section 1 of POPIA, but shall in the context of the Company comprise of the types of Personal Information recorded in this Policy below;

1.26 "**Policy**" means this Data Protection and Privacy Policy;

1.27 **"POPIA"** means the Protection of Personal Information Act, No 4 of 2013;

1.28 **"Processing"** means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information/Personal Data, including:

1.28.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;

1.28.2 dissemination by means of transmission, distribution or making available in any other form by electronic communications or other means; or

1.28.3 merging, linking, blocking, degradation, erasure, or destruction. For the purposes of this definition, "Process" has a corresponding meaning;

1.29 "**Products**" means any goods or items provided by the Company to its Customers;

1.30 "**Regulator**" means the Information Regulator established in terms of POPIA;

1.31 "**Responsible Party**" means in the context of this Policy, the Company;

1.32 "**Services**" means the various services provided by the Company to its Customer(s);

1.33 "**Special Personal Information/Data**" means Personal Information/Personal Data concerning, amongst other aspects contemplated in terms of Section 26 Part B of POPIA, a Data Subject's, religious beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric data, or criminal behaviour;

1.34 "**Third-Party**" means any the Company Group Company (if applicable), Customer(s), Data Subject(s), employees, independent contractor, agent, consultant or user of the Company Products, Services, Website, or any other digital application interface;

1.35 "**Unique Identifier**" means any identifier that is assigned to a Data Subject and is used by the Responsible Party for the purposes of the operations of that Responsible Party and that uniquely identifies that data subject in relation to the Responsible Party;

1.36 "**Website**" means the website owned and operated by the Company sourced at www.digitalecosystems.co.za and

1.37 "**Web Beacons**" means small graphic images called web beacons, also known as "Internet tags" or "clear gifs", which Web Beacons may be deployed in the Company's Website(s) pages and e-mail messages. Web beacons may be invisible to Data Subjects, but any electronic image inserted into a web page or e- mail can act as a Web Beacon. the Company may use web beacons or similar technologies for a number of purposes, including, without limitation, to count the number of visitors to our Websites, Mobile Application(s), to monitor how users navigate the Website(s) or Mobile Application(s), to count how many e-mails that we have sent were actually opened or to count how many particular articles or links were actually viewed by Data Subjects in certain circumstances.

2 INTRODUCTION

2.1 This Policy regulates the Processing of Personal Information/Personal Data by the Company and sets forth the requirements with which the Company undertakes to comply when Processing Personal Information/Personal Data pursuant to undertaking its operations and fulfilling its contractual obligations in respect of Data Subjects and Third Parties in general.

2.2 The Company places a high premium on the privacy of every person or organisation with whom it interacts or engages with and therefore acknowledges the need to ensure that Personal Information/Personal Data is handled with a reasonable standard of care as may be expected from it. The Company is therefore committed to ensuring that it complies with the requirements of POPIA, and also with the terms of the GDPR to the extent that the GDPR applies.

2.3 When a Data Subject or Third Party engages with the Company, whether it be physically or via any digital, electronic interface such as the Company's Website, the Data Subject or Third Party acknowledges that they trust the Company to Process their Personal Information/Personal Data, including the Personal Information/Personal Data of their dependents, beneficiaries, customers, members, or employees as the case may be, which further entrenches the importance of the Company's compliance with Applicable Laws in regards to the Processing of Personal Information/Personal Data.

2.4 All Data Subjects and Third Parties have the right to object to the processing of their Personal Information/Personal Data. It should be voluntary to accept the Terms and Conditions to which this Policy relates. However, the Company does require the Data Subject or Third Party's acceptance to enable the proper use of the Company's Website and/or Services.

3 PURPOSE AND APPLICATION

3.1 The purposes of this Policy are not only to inform Data Subjects of what Personal Information/Personal Data of theirs the Company may Process, where the Company may have collected such Personal Information/Personal Data from (if not directly from them as the Data Subject), how the Company Processes their Personal Information/Personal Data, but also to establish a standard by which the Company and its employees, representatives and operators shall comply in as far as the Processing of Personal Information/Personal Data is concerned.

3.2 The Company, in its capacity as a Responsible Party and/or Operator and/or Controller, as the case may be, shall strive to observe and comply with its obligations under POPIA and the GDPR (as may be applicable and to the extent necessary) when it Processes Personal Information/Personal Data from or in respect of any Data Subject.

4 COLLECTING & PROCESSING OF PERSONAL INFORMATION/PERSONAL DATA

4.1 Whenever any Data Subject engages with the Company, whether it be physically or electronically, or through the use of its Services, facilities or Website the Company will in effect be Processing the Data Subject's Personal Information/Personal Data.

4.2 It may be from time to time that the Company has collected a Data Subject's Personal Information/Personal Data from other sources and in such instances the Company will inform the Data Subject by virtue of any privacy notices it deploys from time to time. In the event that a Data Subject has shared their Personal Information/Personal Data with any third parties, the Company will not be responsible for any loss suffered by the Data Subject, their dependents, beneficiaries, customers, representatives, agents, or employees (as the case may be).

4.3 When a Data Subject provides the Company with the Personal Information of any other Third Party, the Company will process the Personal Information/Personal Data of such Third Party in line with this Policy, as well as any terms and conditions or privacy notices to which this Policy relates.

4.4 The Company will primarily Process Personal Information/Personal Data in order to facilitate and enhance the delivery of Products and/or Services to its Customers, manage and administer its business, foster a legally compliant workplace environment, as well as safeguard the Personal Information/Personal Data relating to any Data Subjects which it in fact holds. In such an instance, the Data Subject providing the Company with such Personal Information/Personal Data may also be required to confirm that they are a Competent Person and that they have authority to give the requisite consent to enable the Company to process such Personal Information/Personal Data.

4.5 The Company undertakes to process any Personal Information/Personal Data in a manner which promotes the constitutional right to privacy, retains accountability and Data Subject participation.

4.6 Prior to recording the purpose(s) for which the Company may, or will, process the Personal Information/Personal Data of Data Subjects, the Company hereby records the types of Personal Information/Personal Data of Data Subjects it may process from time to time:

4.6.1 Full names;

4.6.2 Identity numbers;

4.6.3 Registration numbers;

4.6.4 Financial information, including banking account information;

4.6.5 Statutory information;

4.6.6 Physical and postal address particulars;

4.6.7 Telephone numbers;

4.6.8 Email addresses;

4.6.9 Biometrics;

4.6.10 Unique Identifiers.

4.7 In supplementation of the above and any information privacy notices provided to any Data Subjects from time to time pursuant to any engagement with them, the Company may process Personal Information/Personal Data for the following purposes:

4.7.1 To provide or manage any information, Products and/or Services requested by or delivered to Data Subjects in general;

4.7.2 To establish a Data Subject's needs, wants and preferences in relation to the Products and/or Services provided by the Company;

4.7.3 To help the Company identify Data Subjects when they engage with the Company;

4.7.4 To facilitate the delivery of Products and/or Services to Customers;

4.7.5 To allocate to Customers and Data Subjects Unique Identifiers for the purpose of securely storing, retaining, and recalling their Personal Information/Personal Data from time to time;

4.7.6 To maintain records of Data Subjects and specifically Customer records;

4.7.7 To maintain Third Party records;

4.7.8 For recruitment purposes;

4.7.9 For employment purposes;

4.7.10 For apprenticeship purposes;

4.7.11 For general administration purposes;

4.7.12 For legal and/or contractual purposes;

4.7.13 For health and safety purposes;

4.7.14 To monitor access, secure and manage any facilities owned or operated by the Company regardless of location;

4.7.15 To transact with Third Parties;

4.7.16 To improve the quality of the Company's Services;

4.7.17 To transfer Personal Information/Personal Data to any other Company Group Company so as to enable the relevant Company Group Company to market its products and/or services to the Company's Customer(s) or Third Party's, as well as to render specific services to the Company itself which would in turn enable the Company to render its Services to its Customer(s);

4.7.18 To transfer Personal Information/Personal Data to Third Party service providers, network operators, and original equipment manufacturers (OEM's) so as to enable the Company to deliver its Services or provide its Products to its Customer(s);

4.7.19 To analyse the Personal Information/Personal Data collected for research and statistical purposes;

4.7.20 To help recover bad debts;

4.7.21 To transfer Personal Information/Personal Data across the borders of South Africa to other jurisdictions if it is required;

4.7.22 To carry out analysis and Customer profiling;

4.7.23 To identify other products and services which might be of interest to our Customers and Data Subjects in general, as well as to inform them of such products and/or services;

4.7.24 To comply with any Applicable Laws applicable to the Company.

4.7.25 When collecting Personal Information/Personal Data from a Data Subject, the

Company shall comply with the notification requirements as set out in Section 18 of POPIA, and to the extent applicable, Articles 13 and 14 of the GDPR.

4.8 The Company will collect and Process Personal Information/Personal Data in compliance with the conditions as set out in POPI Act and/or the Processing principles in the GDPR (as the case may be), to ensure that it protects the Data Subject's privacy.

4.9 The Company will not Process the Personal Information/Personal Data of a Data Subject for any purpose other than for the purposes set forth in this Policy or in any other privacy notices which may be provided to Data Subjects from time to time, unless the Company is permitted or required to do so in terms of Applicable Laws or otherwise by law.

4.10 The Company may from time-to-time Process Personal Information/Personal Data by making use of automated means (without deploying any human intervention in the decision-making process) to make decisions about the Data Subject or their application. In this instance it is specifically recorded that the Data Subject may object to or query the outcomes of such a decision.

5 PERSONAL INFORMATION/PERSONAL DATA FOR DIRECT MARKETING PURPOSES

5.1 The Company acknowledges that it may only use Personal Information/Personal Data to contact Data Subjects for purposes of direct marketing where the Company has complied with the provisions of POPIA and GDPR (where applicable) and when it is generally permissible to do so in terms of Applicable Laws.

5.2 In the event that the Company may lawfully direct market to a Data Subject in terms of Section 69 of POPI Act, the Company will ensure that a reasonable opportunity is given to such Data Subjects to object (opt-out) to the use of their Personal Information/Personal Data for the Company’s marketing purposes when collecting the Personal Information/Personal Data and on the occasion of each communication to the Customer for purposes of direct marketing.

6 STORAGE AND RETENTION OF PERSONAL INFORMATION/PERSONAL DATA

6.1 The Company will retain Personal Information/Data it has Processed, in an electronic or hardcopy file format, with a Third-Party service provider appointed for this purpose (the provisions of Clause 9 below will apply in this regard).

6.2 Personal Information/Personal Data will only be retained by the Company for as long as necessary to fulfil the legitimate purposes for which that Personal Information/Personal Data was collected in the first place and/or as permitted or required in terms of Applicable Law.

6.3 It is specifically recorded that any Data Subject has the right to object to the Processing of their Personal Information and the Company shall retain and store the Data Subject's Personal Information/Personal Data for the purposes of dealing with such an objection or enquiry as soon and as swiftly as possible.

7 FAILURE TO PROVIDE PERSONAL INFORMATION

Where the Company is required to collect Personal Information/Personal Data from a Data Subject by law or in order to fulfil a legitimate business purpose of the Company and the Data Subject fails to provide such Personal Information/Personal Data, the Company may, on notice to the Data Subject, decline to render services without any liability to the Data Subject.

8 SECURING PERSONAL INFORMATION/PERSONAL DATA

8.1 The Company will always implement appropriate, reasonable, physical, organisational, contractual and technological security measures to secure the integrity and confidentiality of Personal Information/Personal Data, including measures to protect against the loss or theft, unauthorised access, disclosure, copying, use or modification of Personal Information/Personal Data in compliance with Applicable Laws.

8.2 In further compliance with Applicable Laws, the Company will take steps to notify the relevant Regulator(s) and/or any affected Data Subjects in the event of a security breach and will provide such notification as soon as reasonably possible after becoming aware of any such breach.

8.3 Notwithstanding any other provisions of this Policy, it should be acknowledged that the transmission of Personal Information/Personal Data, whether it be physically in person, via the internet or any other digital data transferring technology, is not completely secure. Whilst the Company has taken all appropriate, reasonable measures contemplated in Clause 8.1 above to secure the integrity and confidentiality of the Personal Information/Personal Data its Processes, in order to guard against the loss of, damage to or unauthorized destruction of Personal Information/Personal Data and

unlawful access to or processing of Personal Information/Personal Data, the Company in no way guarantees that its security system(s) are 100% secure or error-free. Therefore, the Company does not guarantee the security or accuracy of the information (whether it be Personal Information/Personal Data or not) which it collects from any Data Subject.

8.4 Any transmission of Personal Information/Personal Data will be solely at the own risk of a Data Subject. Once the Company has received the Personal Information/Personal Data, it will deploy and use strict procedures and security features to try to prevent unauthorised access to it. As indicated above, the Company reiterates that it restricts access to Personal Information/Personal Data to Third Parties who have a legitimate operational reason for having access to such Personal Information/Personal Data. The Company also maintains electronic and procedural safeguards that comply with the Applicable Laws to protect your Personal Information from any unauthorized access.

8.5 The Company shall not be held responsible and by accepting any terms and conditions to which this Policy relates, any Data Subject agrees to indemnify and hold the Company harmless for any security breaches which may potentially expose the Personal Information/Personal Data in the Company's possession to unauthorized access and or the unlawful processing of such Personal Information/Personal Data by any Third-Party.

9 PROVISION OF PERSONAL INFORMATION/PERSONAL DATA TO THIRD PARTIES

The Company may disclose Personal Information/Personal Data to Third-Party service providers and/or network operator(s) and/or original equipment manufacturers OEM's and/or its business partners where necessary and to achieve the purpose(s) for which the Personal Information/Personal Data was originally collected and processed. The Company will enter into written agreements with such Third-Party service providers and/or network operator(s) and/or original equipment manufacturers OEM's and/or its business partners, to ensure that they comply with Applicable Laws pursuant to the Processing of Personal Information/Personal Data provided to it by the Company from time to time.

10 TRANSFER OF PERSONAL INFORMATION/PERSONAL DATA OUTSIDE OF SOUTH AFRICA

10.1 The Company may, under certain circumstances, transfer Personal Information/Personal Data to a jurisdiction outside of the Republic of South Africa in order to achieve the

purpose(s) for which the Personal Information/Data was collected and processed, including for Processing and storage by Third-Party service providers.

10.2 If it is required, the Company will obtain the Data Subject's consent to transfer the Personal Information/Personal Data to such foreign jurisdiction.

10.3 The Data Subject should also take note that, where the Personal Information/Personal Data is transferred to a foreign jurisdiction, the Processing of Personal Information/Personal Data in the foreign jurisdiction may be subject to the laws of that foreign jurisdiction.

11 ACCESS TO PERSONAL INFORMATION/PERSONAL DATA

11.1 A Data Subject has the right to a copy of the Personal Information/Personal Data which is held by the Company (subject to a few limited exemptions as provided for under Applicable Law).

11.2 The Data Subject must make a written request (which can be by email) to the Information Officer designated by the Company from time to time and whose contact details can be sourced in the Company's PAIA Manual.

11.3 The Company will provide the Data Subject with any such Personal Information/Personal Data to the extent required by Applicable Law and subject to and in accordance with the provisions of the Company's PAIA Manual (published in terms of Section 51 of PAIA, which PAIA Manual can be sourced either at the Company's premises upon request or on the Company's Website.

11.4 The Data Subject can challenge the accuracy or completeness of his/her/its Personal Information/Personal Data in the Company's records at any time in accordance with the process set out in the Company's PAIA Manual.

12 KEEPING PERSONAL INFORMATION/PERSONAL DATA ACCURATE

12.1 The Company will take reasonable steps to ensure that Personal Information/Personal Data that it Processes is kept updated where reasonably possible. For this purpose, the Company shall provide Data Subjects with the opportunity to update their information at appropriate times.

12.2 The Company may not always expressly request the Data Subject to verify and update

his/her/its Personal Information/Personal Data and expects that the Data Subject will notify the Company from time to time in writing:

12.2.1 of any updates or amendments required in respect of his/her/its Personal Information/Personal Data;

12.2.2 where the Data Subject requires the Company to delete his/her/its Personal Information/Personal Data; or

12.2.3 where the Data Subject wishes to restrict the Processing of his/her/its Personal Information/Personal Data.

13 COSTS TO ACCESS PERSONAL INFORMATION/PERSONAL DATA

13.1 In the event that a cost is applicable, the prescribed fees to be paid for copies of the Data Subject's Personal Information/Personal Data are listed in the Company's PAIA Manual.

13.2 The Company reserves the right to make amendments to this Policy from time to time.

14 COMPLAINTS TO THE INFORMATION REGULATOR

14.1 If any Data Subject or Third Party is of the view or belief that the Company has Processed their Personal Information/Personal Data in a manner or for a purpose which is contrary to the provisions of this Policy, the Data Subject is requested to first attempt to resolve the matter directly with the Company, failing which the Data Subject or Third Party shall have the right to lodge a complaint with the Information Regulator, under the provisions of POPIA.

14.2 The current contact particulars of the Information Regulator are:

The Information Regulator (South Africa)
Website: **https://www.justice.gov.za/inforeg/index.html**
Woodmead North Office Park 54 Maxwell Drive. Woodmead, Johannesburg, 2191.PO Box 31533 Braamfontein, Johannesburg,2107.

15 CONTACTING US

All comments, questions, concerns or complaints regarding Personal Information/Personal Data or this Policy, should be forwarded to the Company's Information Officer at the following email johan@digitalecosystems.co.za