

PAIA AND POPIA MANUAL

Prepared in terms of:

**Section 51 of the Promotion of Access to Information Act 2 of 2000
(as amended)**

and

Section 14 of the Protection of Personal Information Act of 2013

of

**Bureau van Dijk Electronic Publishing
S.A. (Pty.) Ltd.**

**DATE OF COMPILATION: 14/12/2022
DATE OF LAST REVISION: 01/2/2024**

1. DEFINITIONS AND INTERPRETATIONS

- 1.1 **“Company”** means Bureau van Dijk Publishing S.A. (Pty) Ltd;
- 1.2 **“Data Subject”** has the meaning ascribed thereto in Section 1 of POPIA being the person to whom personal information relates to;
- 1.3 **“Employee”** refers to any person who works for the Company;
- 1.4 **“Information Regulator”** as established in terms of section 39 of the PAIA, 2013, to independently exercise certain powers and to perform certain duties and functions, i.e., provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith. The Information Regulator is accountable to the National Assembly; **“PAIA”** means the Promotion of Access to Information Act No. 2 of 2000, as Amended;
- 1.5 **“Personal Information”** has the meaning ascribed thereto in Section 1 of POPIA being information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person such as a company. Personal information is any information that can be used to reveal a person's or entity's identity;
- 1.6 **“POPIA”** means the Protection of Personal Information Act No.4 of 2013;
- 1.7 **“Record”** has the meaning ascribed thereto in Section 1 of PAIA, being any recorded information, regardless of its medium or form;
- 1.8 **“Requester”** has the meaning ascribed thereto in Section 1 of PAIA, being, in relation to
 - (a) a public body, means
 - (i). Any person (other than a public body contemplated in paragraph (a) or (b)(i) of the definition of “public body”, or an official thereof) making a request for access to records of that public body; or
 - (b) a private body, means
 - (i) any person, including but not limited to, a public body or an official thereof, making a request for access to a record of that private body;

Capitalised terms used in this PAIA Manual have the meanings ascribed thereto in Section 1, of this manual, of POPIA and PAIA as the context specifically requires, unless otherwise defined herein.

2. PURPOSE OF PAIA and PAIA MANUAL

2.1 In terms of PAIA:

This Manual, in terms of Section 14 of PAIA is for the purpose of:

- 1.1.1. checking the categories of Records held by the Company;
- 1.1.2. having a sufficient understanding of how to make a request for access to a Record of the Company, by providing a description of the categories of Records which the Company holds;
- 1.1.3. accessing the relevant contact details of the Information Officer who will assist the public with the Records they intend to access;
- 1.1.4. knowing the description of the guide on how to use PAIA, as updated by the Regulator and how to obtain access to it;
- 1.1.5. knowing if the Company processes Personal Information, and if so, the purpose of processing of Personal Information, the description of the categories of Data Subjects and of the information or categories of information relating thereto,
- 1.1.6. knowing the recipients or categories of recipients to whom the Personal Information may be supplied,
- 1.1.7. knowing whether the company has planned to transfer or process Personal Information outside of the Republic of South Africa,
- 1.1.8. knowing whether the company has security measures to ensure the confidentiality, integrity and availability of the Personal Information processed.

2.2 In terms of PAIA:

This Manual's, in terms of Section 17 of POPIA, purpose is:

- 2.2.1 to encourage compliance with POPI;
- 2.2.2 to inform stakeholders and data subjects of the compliance associated with POPIA, which includes:
 - breaches of confidentiality;
 - failing to offer choice; and
 - reputational damage

3. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF THE COMPANY

3.1. The Company

Full Name: Bureau van Dijk Publishing S.A. (Pty.) Ltd
Registration Number: 2010/018794/07
Registered Address: Nelson Mandela Square, 2nd Floor, West Tower, Maude Street, Sandton, 2196, Johannesburg, South Africa
Tel: Contact Information Officer
Email: Contact Information Officer

3.2. Information Officer

Name: Deidre de Carvalho
Tel: 082 659 8594
Email: deidre@randco.co.za

4. AVAILABILITY OF PAIA MANUAL

4.1. This PAIA Manual is available for inspection during office hours from the Information Officer, free of charge, or by email from Moody's Privacy Team (privacy@moodys.com).

5. THE INFORMATION REGULATOR'S OFFICIAL GUIDE

5.1 The Guide that has been published contains the following information:

- a) the object of PAIA;
- b) particulars of the information;
- c) the manner and form of a Request to information held by a Private Body;
- d) assistance available from both the Information Officer and the Information Regulator in terms of PAIA;
- e) all remedies in law regarding acts, omissions, rights and duties, including how to lodge an internal appeal, a complaint to the regulator and a court application;
- f) schedules of fees to be paid in relation to requests for access to information, and regulations made in terms of PAIA.

5.2. A copy of the PAIA Guide is available for inspection at the offices of the Information Regulator situated at 27 Stiemens Street, Braamfontein, Gauteng, South Africa and on the website at info regulator.org.za . Contact details are as follows:

Post: Information Regulator (South Africa), PO Box 31533, Braamfontein, 2017
 Telephone: 010 023 5287
 Website: info regulator.org.za
 E-mail: enquiries@info regulator.org.za

6. CATEGORIES OF RECORDS OF THE COMPANY

6.1. The Company holds the following categories of information which will be available for inspection in terms of PAIA. The procedure in terms of which such Records may be requested from the Company is set out in Section 8 of this Manual. The Records listed below will not in all instances be provided to a Requestor who requests them in terms of PAIA, as the Requestor is required to identify the right the Requestor is seeking to exercise or protect and provide an explanation of why the requested Record is required for the exercise or protection of that right. Furthermore, the request may be denied on the basis of the grounds of refusal under PAIA.

Category of Records	Description of Records
Statutory information/records	<ul style="list-style-type: none"> • Records of minutes, as well as resolutions passed (where applicable) • Memorandum & articles of association, copies of all forms lodged with the CIPC • Directors register • Company Registers
Financial records (where applicable)	<ul style="list-style-type: none"> • Tax records • Accounting records • Debtors' records • Creditors' records • Insurance records • Auditors' reports • Interim and annual financial statements • Bank statements and other banking records

Category of Records	Description of Records
	<ul style="list-style-type: none"> • Invoices issued in respect of debtors and billing information • Records regarding the company's financial commitments.
Statutory employee records including internal policies and procedures	<ul style="list-style-type: none"> • Personnel records of Employees • Conditions of employment • Employment contracts • Employment policies and procedures • Remuneration paid to each Employee • Salary and wage register and other payroll records • Registrations with Department of Labour, Unemployment Insurance Fund, Compensation Fund and in terms of the Skills Development Levies Act • Records of Unemployment Insurance Fund contributions • Records regarding group life assurance and disability income protection • Health and safety records • Workplace skills plans • Training schedules and material.
The Company's subsidiary/ holding/affiliate companies	<ul style="list-style-type: none"> • Company information, including company registration number, registered office address, shareholders and directors.
Clients and client's subsidiary/ holding/affiliate companies	<ul style="list-style-type: none"> • Company information, including company registration number, registered office address • Transaction history.
The Company's suppliers, vendors and contractors	<ul style="list-style-type: none"> • Company information, including company registration number, registered office address • Transaction history.
Companies and individuals associated with companies, such as directors and shareholders	<ul style="list-style-type: none"> • Name and contact details • Date/year of birth, nationality, national ID

Category of Records	Description of Records
	<ul style="list-style-type: none"> • Biography, directorship details, positions held within companies.
Third parties involved in any litigation, dispute, or transaction with	<ul style="list-style-type: none"> • Name and contact details • Company information, including company registration number, registered office address • Details of the litigation, dispute or transaction
Assets	<ul style="list-style-type: none"> • Fixed asset register (where applicable) • Moveable asset register (where applicable).
Agreements and contracts	<ul style="list-style-type: none"> • All agreements of a material nature
Administration, secretarial and legal records (where applicable)	<ul style="list-style-type: none"> • Complaints, pleadings, briefs and other documents pertaining to any actual, pending or threatened litigation, arbitration or investigation • Settlement agreements • Shareholder records • Share register • Minutes of meetings of directors • Records relating to the incorporation of the Company • Minutes of meetings of committees and sub-committees • Powers of attorney • Records of litigation / arbitration proceedings • Title deeds • Mortgage bonds; • Trademark, copyright, patent, service mark certificates and registrations • Material licences, permits and authorisations.
Insurance	<ul style="list-style-type: none"> • Insurance policies • Claim records • Details of insurance coverage, limits and insurers.
Information Technology	<ul style="list-style-type: none"> • Hardware • Operating systems and other operational Records • Telephone and other lines • Software packages • Agreements • Support and maintenance agreements • User manuals and licences.
Sales and marketing	<ul style="list-style-type: none"> • Sales, advertising, promotional and marketing materials

7. DESCRIPTION OF THE RECORDS OF THE COMPANY WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION

The following information is available in terms of the following legislation, persons or entities specified in such legislation:

- 7.1. Basic Conditions of Employment Act, No. 75 of 1997
- 7.2. Companies Act, No. 71 of 2008
- 7.3. Compensation for Occupational Injuries and Diseases Act, No.130 of 1993
- 7.4. Constitution of the Republic of South Africa 2008
- 7.5. Copyright Act No 114 of 1998
- 7.6. Debt Collectors Act, No. 114 of 1998
- 7.7. Electronic Communications Act No. 36 of 200
- 7.8. Electronic Communications and Transactions Act, No. 25 of 2002
- 7.9. Employment Equity Act, No. 55 of 1998
- 7.10. Financial Intelligence Centre Act, No. 38 of 2001
- 7.11. Income Tax Act, No. 58 of 1962
- 7.12. Labour Relations Act, No. 66 of 1995
- 7.13. Legal Practice Act No 28 of 2014
- 7.14. National Credit Act. 34 of 2005
- 7.15. Medical Schemes Act, No. 131 of 1998
- 7.16. Occupational Health & Safety Act, No. 85 of 1993
- 7.17. Pensions Fund Act, No. 24 of 1956
- 7.18. Promotion of Access to Information Act No. 2 of 2000
- 7.19. Protection of Personal Information Act, No. 4 of 2013
- 7.20. Skills Development Act, No. 97 of 1998
- 7.21. Skills Development Levies Act, No. 9 of 1999
- 7.22. Tax on Retirement Funds Act, No. 38 of 1996
- 7.23. Unemployment Insurance Act, No. 63 of 2001
- 7.24. Unemployment Insurance Contributions Act, No. 4 of 2002
- 7.25. Value Added Tax Act, No. 89 of 1991

Note, whilst all reasonable endeavours have been made to provide a complete list of applicable legislation above, it is possible that the above list may be incomplete. Wherever it comes to the Company's attention that existing or new legislation allows a Requestor access on a basis other than that set out in the Act, the above list will be updated.

- 8. PROCEDURE FOR REQUESTING ACCESS TO INFORMATION IN TERMS OF PAIA**
- 8.1.** A request must comply with all the procedural requirements as contained in section 53 of PAIA relating to a Request for Access to a Record.
 - 8.2.** The Company will process the Request for Access and notify the Requestor of the decision within 30 days of receipt of the Request for Access, unless the Request for Access is of such a nature that an extension of the prescribed time limit is necessitated in accordance with section 57 of PAIA. In the case of an extension of the time limit, the Requestor has the right to lodge a complaint with the Information Regulator in accordance with PAIA and POPIA by completing the prescribed forms.
 - 8.3.** There are various grounds upon which the Company may or must refuse a Request for Access to a Record in accordance with Chapter 4 of PAIA.
 - 8.4.** Requests for information that are clearly frivolous or vexatious, or which involve unreasonable diversion of resources shall be refused.
 - 8.5.** All requests for information will be assessed on their own merits and in accordance with applicable laws.
 - 8.6.** Once the Information Officer has heard all the submissions, he or she will decide as to whether or not access to the Record will be granted. If access is granted the Requestor must then be granted access to the Record within 30 days of being informed of the decision.
 - 8.7.** If the request for access is successful, an access fee may be required for the search, reproduction and/or preparation of the Record(s). The access fee must be paid prior to access being given to the requested Record(s).
 - 8.8.** If the Information Officer does not grant the Requestor access to the Record the Requestor is entitled in accordance with sections 56(3) (c) and 78 of PAIA to apply to a court for relief within 180 days of notification of the decision for appropriate relief, such as an order compelling the Record or Records requested to be made available to the Requestor or for another appropriate order. The court will determine whether the records should be made available or not.
 - 8.9.** The Requestor may also approach the Information Regulator and lodge a complaint in accordance with section 74 of POPIA in the prescribed form and email to: POPIAComplaints@inforegulator.org.za and in accordance with section 77(a) of PAIA and email to: PAIAComplaints@inforegulator.org.za.
 - 8.10.** If a requested record cannot be found or if the records do not exist, the Information Officer shall, by way of an affidavit or an affirmation, notify the Requestor that it is not possible to give access to the requested record.

9. PURPOSES OF PROCESSING PERSONAL INFORMATION

9.1. The purposes for which the Company Processes Personal Information are:

- 9.1.1. Engaging in commercial transactions with clients, vendors and other business contacts;
- 9.1.2. To offer products and services to clients;
- 9.1.3. To manage the Company's relationship with its Employees;
- 9.1.4. For the performance of marketing activities;
- 9.1.5. In order to comply with laws, regulations, court orders, judgements and other legal obligations;
- 9.1.6. As may be necessary for pursuing the Company's legitimate interests or that of a third party to whom the Personal Information is disclosed;
- 9.1.7. To protect the Company's rights or property;
- 9.1.8. As necessary to protect someone's health, safety or welfare; and
- 9.1.9. In other ways to which the Data Subjects' consent.

10. DESCRIPTION OF THE CATEGORIES OF DATA SUBJECTS

10.1. As per section 1 of POPIA, a Data Subject may either be a natural or a juristic person. The categories of Data Subjects and types of Personal Information the Company Processes include, but are not limited to:

Categories of Data Subjects	Categories of Personal Information
The Company's Employees	<ul style="list-style-type: none"> • Name and contact details • Employee identification number, social security number, passport details, residency/work permit details, driver's license information • Date of birth, gender, nationality, language(s), next of kin • Details of employment, including compensation, performance, benefits, stock grants, banking details, tax details, working time records, job title, work history, disciplinary records, performance evaluations, learning programs, biographies

Categories of Data Subjects	Categories of Personal Information
	<ul style="list-style-type: none"> • User ID, IP address, computer details, accounts, passwords, access logs, activity logs, communications, CCTV video recordings in office public spaces, ID badge entry records, health and safety records • Sensitive information such as health/medical information.
Candidates	<ul style="list-style-type: none"> • Name and contact details • Application data, including resume/CV data • Background check details.
Office visitors	<ul style="list-style-type: none"> • Name and company details • CCTV video recordings in office public spaces.
Web visitors	<ul style="list-style-type: none"> • IP address • Cookie data • Form fill data.
The Company's subsidiary/holding/affiliate companies	<ul style="list-style-type: none"> • Company information, including company registration number, registered office address, shareholders and directors.
Clients and client's subsidiary/holding/affiliate companies	<ul style="list-style-type: none"> • Company information, including company registration number, registered office address • Transaction history.
The Company's suppliers, vendors and contractors	<ul style="list-style-type: none"> • Company information, including company registration number, registered office address • Transaction history.
Companies and individuals associated with companies, such as directors and shareholders	<ul style="list-style-type: none"> • Name and contact details • Date/year of birth, nationality, national ID • Biography, directorship details, positions held within companies.
Third parties involved in any litigation, dispute, or transaction with	<ul style="list-style-type: none"> • Name and contact details • Company information, including company registration number, registered office address • Details of the litigation, dispute or transaction

11. RECIPIENTS OF THE PERSONAL INFORMATION

11.1. The recipients or categories of recipients to whom the personal information may be supplied include, but are not limited to:

- 11.1.1. Affiliates;
- 11.1.2. Auditors;
- 11.1.3. Clients;
- 11.1.4. Service providers;
- 11.1.5. Business partners;
- 11.1.6. Regulatory authorities, government bodies or agencies, judicial bodies.

12. TRANSBORDER FLOWS OF PERSONAL INFORMATION

12.1. The Company transfers Personal Information outside the Republic of South Africa including, but not limited to:

- 12.1.1. Company headquarters in the United States;
- 12.1.2. Personal Information stored on internal systems hosted in the United States and accessible by affiliates globally;
- 12.1.3. Service providers located in the United States and elsewhere;
- 12.1.4. Clients located globally;
- 12.1.5. Regulators and courts located globally.

13. DATA MANAGEMENT

13.1. Security Breaches and Incident Management

In an event where personal information of a data subject is compromised and accessed unlawfully it is the responsible party's (the company's) responsibility to notify the Information Regulator as well as the affected parties as soon as reasonably possible.

The act does however take into account delayed notifications of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determined that notification would impede on a criminal investigation by the public body concerned.

The company can launch an investigation, if not being investigated by a public body, into the cause of the breach and assess the risk whilst implementing mitigating factors to prevent future breaches.

A data breach action plan includes, but are not limited to, the following:

1. All parties related to the incident will assist one another to attend to a breach as soon as possible with maximum allowed force.
2. When an incident occurs, the incident, in compliance with the POPI Act will not be discussed with anyone but the employee's direct manager.

3. Managers may only discuss incidents with the Information Officer.
4. The Information Officer may only discuss the matter with the board of directors, whereafter the board will direct the CEO.
5. Once a breach is confirmed, the Information Officer will communicate, as prescribed by the POPI Act, with the affected data subject, the Regulator and the those who may be influenced by the breach.
6. The following will be documented:
 - a. All risks, incidents, and threats.
 - b. All responses to the above.
 - c. Details of the breach, i.e., time, place, format of data, size of breach, reasons and possible consequences, etc.
 - d. An action plan to remedy the breach with the roles and responsibilities of all parties related to the matter.
 - e. The Company has forms and written procedures for all steps related to the stages of breach.

13.2. Security Measures

The Company implements appropriate information security measures to safeguard the confidentiality, integrity and availability of the information include, but are not limited to:

- 13.2.1. A comprehensive written information security program, including policies, procedures and training;
- 13.2.2. Physical security measures including secure business facilities and data centres;
- 13.2.3. Technical security measures including encryption, multi-factor authentication, access controls, firewalls, audit logs, monitoring reports, patch management, vulnerability management;
- 13.2.4. Administrative controls, including role-based access, pre-employment screening, confidentiality obligations on Employees, formal disciplinary processes in the event that any Employee violates their confidentiality obligations.

13.3. Disciplinary Action

Some of the immediate action that can be taken subsequent to an investigation also include referral to **law enforcement agencies** where criminal charges can be made, **disciplinary action** or the **recovery of funds and assets** in order to restrict any prejudice or damages caused.

Once an investigation has been completed on an infringement or complaint, the company may recommend any appropriate administrative, legal and/or disciplinary action to be taken against the relevant employee reasonably suspected of being implicated in any non-compliant activity outlined within this manual.

Any willful mismanagement of personal information or gross negligence will be considered a serious form of misconduct and the company may summarily dismiss the employee. Disciplinary procedures will begin where sufficient evidence was found to support the gross negligence of personal information by an employee.

14. COMPLAINTS TO THE INFORMATION REGULATOR

The Requestor may also approach the Information Regulator and lodge a complaint in accordance with section 74 of POPIA and section 77(a) of PAIA in the prescribed form.

The prescribed complaints form can be sent to:

POPIAComplaints@infoeregulator.org.za, and

PAIAComplaints@infoeregulator.org.za

A requester or third party may only submit a complaint to the Regulator after that requester or third party has exhausted the internal appeal procedure against a decision of the Information Officer of a public body or head of private body.

15. UPDATING OF THE MANUAL

The Information Officer will review and amend, as required, this PAIA Manual on a regular basis.

Issued by Deidre de Carvalho

Information Officer

Bureau van Dijk Electronic Publishing S.A. (Pty.) Ltd.

1 February 2024