

PAIA Manual: Promotion of Access to Information Act

Section
1. List of Acronyms and Abbreviations
2. Purpose of the PAIA Manual
3. Introduction
4. Contact Details and Information
5. Purpose of Processing Personal Information
6. Records of Applicable Legislation which are Available in Accordance with any Other Legislation
7. Category of Records of Aurora Insurance Company Limited
8. General Security Measures Implemented by the Responsible Party to Ensure Confidentiality, Integrity and Availability of the Information
9. The Following needs to be Considered before Submission of a Request for Information
10. Access to Records Held by Aurora Insurance Company Limited
11. The request procedures
12. Grounds for Refusal of Access to Records
13. Remedies
14. Updating of the Manual
15. Availability of the manual

1. List of Acronyms and Abbreviations

"Aurora Insurance Company Limited"	Aurora
"Data Subject" (as defined in POPIA)	Person to whom the personal information relates
"IO"	Information Officer
"Minister"	The Cabinet member responsible for the administration of justice.
"PAIA"	Promotion of Access to Information Act No. 2 of 2000 (as Amended)
"POPIA"	Protection of Personal Information Act No.4 of 2013

“Private Body”	Means: • A natural person who carries or has carried on any trade, business or profession, but only in such capacity. • A partnership which carries or has carried on any trade, business or profession. • Any former or existing juristic person ; or • A Political party. But excludes a public body.
“Regulator”	Information Regulator of South Africa,
“Republic”	The Republic of South Africa
“Responsible Party”	A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information. The Public Body in this case is Aurora Insurance Company Limited.
“The Company”	Aurora Insurance Company Limited.

2. Purpose of the PAIA Manual

- 2.1 This guide to accessing records held by Aurora is intended to provide guidelines to members of the public who wish to exercise their constitutional and statutory right to access information.
- 2.2 Below is information on how to submit a request, a description of the types of records that will be made available, grounds for refusal, what procedure will be followed in considering a request, the applicable fee structure and information on the appeals procedure should the outcome of a request not satisfy the requester.

3 Introduction

- 3.1 Aurora Insurance Company (The Company) conducts business as a licensed non-life insurance company. The Company is a registered financial services provider with the Financial Sector Conduct Authority (FSCA). Our FSP license number is: 34877.
- 3.2 The Promotion of Access to Information Act, No. 2 of 2000 (“the Act”) gives effect to the Constitutional right of access to any information in records held by private bodies that is required for the exercise or protection of any rights. The Act grants a requester access to records of a private body, if the record is required for the exercise or protection of any rights. If a public body lodges a request, the public body must be acting in public interest. The Act sets out the requisite procedural issues attached to a request for access to information, the requirements which such request must meet as well as the grounds for refusal or partial refusal of such request.
- 3.3 This manual informs requesters of procedural and other requirements which requests must meet as prescribed by the Act.

- 3.4 The Act recognises that the right to access to information cannot be unlimited and should be subject to justifiable limitations, including, but not limited to limitations aimed at the reasonable protection of privacy, commercial confidentiality, and effective, efficient and good governance in a manner which balances that right with any other rights, including such rights contained in the Bill of Rights in the Constitution.

4 The details of the company are as follows:

The Company	Aurora Insurance Company Limited
Registration number	2008/003335/06
Physical Address	47 Corlett Drive Illovo Ext 1 Sandton 2196
Registered Address	47 Corlett Drive Illovo, Ext 1 Sandton 2196
Main Business	Insurance
Information Officer	Alida Johanna Botha
Address	47 Corlett Drive, Illovo, Ext 1, 2196
Telephone	+27 11 885 6687

5 Contact details and information:

- 5.1 All requests for access to records in terms of the Act must be in writing and must be addressed to the Information Officer at the contact details noted above:

6 Purpose of processing Personal Information:

- 6.1 The Company collects personal information to be able to provide financial services for the marketing and assisting individuals with the financial services product requirements. The Company also processes personal information for employment of staff and outsourcing of specialised services.

7 Records of Applicable Legislation which are Available in Accordance with any Other Legislation:

- 7.1 A table of legislation setting out a description of the records of the Company which are available in accordance with other legislation:

	Category of records	Applicable legislation
No	Ref	Act
1	No. 61 of 1973	Companies Act
2	No 71 of 2008	Companies Act
3	No 95 of 1967	Income Tax Act
4	No 66 of 1995	Labour Relations Act
5	No 89 of 1991	Value Added Tax Act

	Category of records	Applicable legislation
6	No 75 of 1997	Basic Conditions of Employment Act
7	No 25 of 2002	Electronic Communications and Transactions Act
8	No 2 of 2000	Promotion of Access of Information Act
9	No 54 of 2002	Promotion of Access of Information Amendment Act
10	No 30 of 1996	Unemployment Insurance Act
11	No 78 of 1998	National Payment System Act
12	No 38 of 2001	Financial Intelligence Centre Act
13	No 85 of 1993	Occupational Health and Safety Act
14	No 9 of 1999	Skills Development Levies Act
15	No 4 of 2013	Protection of Personal Information Act
16	No 26 of 2000	Protected Disclosures Act
17	No 130 of 1993	Compensation for Occupational Injuries and Diseases Act
18	No 12 of 2004	Prevention and Combating of Corrupt Activities Act
19	No 53 of 2003	Broad Based Black Economic Empowerment Act
20	No 36 of 2005	Electronic Communications Act
21	No 37 of 2002	Financial Advisory and Intermediary Services Act
22	No 68 of 2008	Consumer Protection Act
23	No 55 of 1998	Employment Equity Act
24	No 18 of 2017	Insurance Act
25	No 34 of 2005	National Credit Act
26	No 68 of 1969	Prescription Act
27	No. 66 of 1965	Administration of Estates Act
28	No 53 of 2003	Financial Sector Charter Code of the Broad-based Black Economic Empowerment Act
29	No. 97 of 1990;	Financial Services Board Act
30	No. 9 of 2017	Financial Sector Regulation Act
31	No. 24 of 1936	Insolvency Act
32	No. 53 of 1998	Short-term Insurance Act
33	No. 97 of 1998	Skills Development Act
34	No. 28 of 2011	Tax Administration Act
35	No. 57 of 1988	Trust Property Control Act
36	No. 4 of 2002	Unemployment Insurance Contributions Act

8 Category of Records of the Company:

- 8.1 The Company has under its control or in its possession the following categories of records under the subjects described below. The categories of records are not exhaustive and are subject to amendment from time to time. A request made for access to these records will not automatically be granted but will be evaluated in accordance with the provisions of the Act, any other legal requirements, and the Company's policies.

Category of record	Type of record	Available on request
Governance & FAIS Disclosures	• Complaints Management Framework • Claims Framework • Conflict of Interest Policy • Treating Customers Fairly Policy • PAIA Manual • Disclosure Document • Compliance framework • BCM – Immediate Cyber Response Plan • BCM – Disaster Recovery Plan • BCM – Governance Policies • BCM – Crisis Management Plan – Operations • BCM – Crisis Management Plan – Cybersecurity • BCM – Business Continuity Plan • BCM- Business Impact Analysis • Fit and Proper Policy • POPIA and Data Management Policy • Code of Conduct and Company Ethics • Money Laundering and Fraud Policy • Human Resource policy • Overall Risk Management Framework • Business Continuity Policy – Legal and Finance • Record Keeping Policy • Internal Control Policy • Remuneration Policy • Debarment Policy • Advertising Policy • Outsourcing Policy	X
Marketing	• Product offerings • External newsletters and circulars • Internal newsletters and circulars • Information on the company published by third parties	X

8.2 Subjects on Which the Company Holds Records

Subjects on which Aurora holds records	Categories of records
Company Secretarial Records	• Company incorporation documents • Names and details of directors • Names and details of shareholders • Salaries of directors
Financial	• Financial statements • Management accounts • Financial and Tax records (Company & Employee) • Asset Register • Statutory returns • Financial agreements • Banking details
Human Resources	• HR policies, procedures and records • Statutory Employee records • Performance records • Key Individual and Representative register • Payroll records • Recruitment and Termination • List of employees • Personal information of employees • Employee contracts • Leave records

	• Code of Conduct • Internal records and correspondence • Internal disciplinary and grievance procedures • Training records
Insurance of Company	• Insurance policies held by the company • Asset register
Marketing	• Customer/policyholder database • Product offering documentation • Marketing material
Client Records	• Key Individual & Representative Registers • Accounts • Monitoring Reports • Financial Statements • Documented policies and procedures • Profile changes • CIPC documents • Licence certificates • Qualifications • Complaints • Contact details of individuals within customer's/policyholder's base • Communications with customers/policyholders
Company Policies and Directives	• Internal relating to employees and the company • External relating to clients and other third parties
Agreements or Contracts	• Standard agreements • Contracts concluded with customers/policyholders • NDAs • Third party contracts such as SLA's, other agreements etc.) • Office management contracts • Supplier contracts • Outsource agreements
Regulatory	• Licenses or Authorisations

8.3 Categories of Data Subjects and Information

Categories of Data Subjects	Types of Personal Information Processed
Customers/policyholders / Liquidators / Curators / Trustees / Executors / Master's Office / Service Providers / Clients	Name, surname, address, registration numbers, identity numbers, identity documents, bank details, cellphone numbers, email addresses, financial statements, application forms, VAT numbers, Telephone numbers, website address, credit history, qualifications.
Service Providers	Names, registration numbers, VAT numbers, Address, email address, cellphone numbers, Telephone numbers and bank details
Employee/s	Name, surname, email address, contact details, physical Address, qualifications, CV's, gender, race, identity numbers, passport numbers, bank account details, leave records, medical notes.

8.4 The Recipients or Categories of Recipients to Whom Personal Information May be Supplied

Category of personal information	Recipients or Categories of Recipients to whom the personal information may be supplied
ID and / or passport numbers	Regulatory Authorities in South Africa – Financial Services Conduct Authority (FSCA), Prudential Authority (PA), South Africa Revenue Services (SARS) Financial Services Providers (FSPs), Department of Labour (DL), Accounting service provider, Verification agencies
Email address	Marketing service provider, FSCA, PA, Accounting service providers, clients
VAT numbers	SARS, Accounting service provider
Payroll	Payroll service provider, Banks
Representative Registers	FSCA, FSPs
Company Registration numbers	FSCA, PA, CIPC, Accounting service providers
Telephone and Cellphone Numbers	FSCA, PA, FSPs, CIPC, Accounting service providers
Addresses	FSCA, PA, SARS, Accounting service providers
Bank Account details for payment details and FAIS Registration	Clients, FSCA, PA, Accounting service providers
FSP service providers (accounting officers and auditors)	FSCA, PA

9. General Security Measures Implemented by the Responsible Party to Ensure the Confidentiality, Integrity and Availability of the Information:

9.1 The main data related risks the Company faces are the regulatory obligations to hold data and the compromising of client data. This risk is addressed in various ways, as outlined below.

9.2 The Company faces various types of risk each day, from natural, technical, human, operational, reputational, procedural, project, financial, political and other sources, sometimes from highly unpredictable sources.

9.3 Whilst it is not possible to avoid these risks in its everyday trading environments, a formal risk management process assists senior management assessing these risks and making decisions as to what actions are required to minimize potential disruptions. These processes pre-define (as far as possible) the actions that are necessary and the resources that are needed to achieve its objectives. The actions outlined within these processes are not intended to cover every eventuality, as all events and crises are unique.

9.4 To safeguard personal information, the Company has implemented various state-of-the-art security measures and ensures these are maintained and upgraded. The main data related risk the Company faces is comprising of client data and this risk is addressed in various ways, as outlined below:

9.4.1 Building access controls are limited to trusted individuals.

9.4.2 Wi-Fi separation ensures that wireless devices cannot access the core network.

9.4.3 Operator logins are changed regularly and are stored on a domain controller.

9.4.4 Credential separation forces VPN users to connect with an unusual username/password.

- 9.4.5 Connections to company databases can only be made using encrypted connection strings.
- 9.4.6 Older database backups are kept in protected archives.
- 9.4.7 Firewalls are in place to shield the entire system.
- 9.4.8 Highly confidential data resides in highly restricted areas.
- 9.4.9 Confidential company data is accessible only to data workers of that company.
- 9.4.10 Only a limited number of data workers can generate reports.
- 9.4.11 System operators don't have access to online mail providers like Gmail, Yahoo etc.
- 9.4.12 A Mail tracker holds a record of all mail flow into and out of the company.
- 9.4.13 User access to USB storage devices is restricted.
- 9.4.14 Regular alerts are sent to staff to educate them in spotting potential malware attacks.
- 9.4.15 Protection of client data on external systems:
 - 9.4.15.1 Access to the recordings of voice conversations is restricted to system administrators.
 - 9.4.15.2 No client information is stored with any of the cloud providers (Dropbox, OneDrive etc.).
 - 9.4.15.3 Data is only exchangeable with external contractors using secure FTP sites.
 - 9.4.15.4 Daily data backup disks are encrypted, rendering them useless in the hands of strangers.
 - 9.4.15.5 The company's mail server makes only encrypted connections to the mail service provider to protect mail flow, both in and out.
 - 9.4.15.6 Aggressive spam filters are in place to limit exposure to malware.

10 General Security Measures Implemented by the Responsible Party to Ensure the Confidentiality, Integrity and Availability of the Information:

10.1 Is the Request Submitted to Exercise or Protect a Requester's Legitimate Rights?

- 10.1.1 The exercise of a requester's rights is subject to justifiable limitations, including the reasonable protection of privacy, commercial confidentiality, and effective, efficient and good governance. This legislation may not be used for access to a record for criminal or civil proceedings or requested after the commencement of such proceedings.
-

10.2 Is the Information Under the Control of the Company?

10.2.1 The Act only applies to records that have already been created, at the date of the request, and that are under the control of the Company. The Company is not obliged to retrieve any records on behalf of a requester that are no longer under its control, even where the Company created the record.

10.3 Does the Requester have a Legitimate Right to Access the Record?

10.3.1 A request may only be made to exercise a requester's own right, or where the request is made on behalf of another person, the requester must submit proof of their capacity to act on behalf of the person in whose name the request is made.

11. Access to Records Held by The Company

11.1 Records held by the Company may be accessed by requests only once the prerequisite requirements for access have been met.

11.2 A requester is any person making a request for access to a record of the Company. There are two types of requesters:

11.2.1 Personal Requester

11.2.1.1 A personal requester is a requester who is seeking access to a record containing personal information about the requester.

11.2.1.2 Subject to the provisions of the Act and applicable law, the Company will provide the requested information, or give access to any record about the requester's personal information. The prescribed fee for reproduction of the information requested will be charged, where applicable.

11.2.2 Other Requester

11.2.2.1 This requester (other than a personal requester) is entitled to request access to information on third parties. However, the Company is not obliged to grant access unless the law allows for it and the requester has a legitimate and reasonable interest in the information. The requester must fulfil the prerequisite requirements for access in terms of the Act, including the payment of a request and access fee.

12. The Request procedures

12.1 The following procedural requirements serve as guidelines for requesters:

12.1.1 The requester must also comply with all the procedural requirements contained in the Act relating to the request for access to a record.

12.1.1.1 Form of request:

- 12.1.1.1.1 To make the request for access to a record, the requester must complete the prescribed form as well as make payment, if applicable. This must be made to the IO of the Company. This request must be made to the address, or electronic mail address detailed above.
 - 12.1.1.1.2 The requester must provide sufficient detail on the request form to enable the IO of the Company to identify the following:
 - 12.1.1.1.2.1 Record or records requested
 - 12.1.1.1.2.2 The identity of the requestor
 - 12.1.1.1.2.3 Which form of access is required, if the request is granted
 - 12.1.1.1.2.4 The requester (and if an agent is lodging the request, proof of capacity)
 - 12.1.1.1.2.5 The postal address or fax number of the requester (where applicable)
 - 12.1.1.1.3 The requester must identify the right that is sought to be exercised or to be protected and provide an explanation of why the requested record is required for the exercise or protection of that right.
 - 12.1.1.1.4 If a request is made on behalf of another person, the requester must then submit proof of the capacity in which the requester is making the request to the satisfaction of the IO of the Company.
 - 12.1.1.1.5 Subject to the provisions in the Act in respect of extensions, the Company will process the request within 30 days, unless the requester has stated special reasons which would satisfy the IO that circumstances dictate that the above time periods not be complied with.
 - 12.1.1.1.6 The Company shall respond to the requester (and provide the requested documents) according to the manner of communication indicated by the requester in its application, which will then be deemed to be received/collected by the requester.
 - 12.1.1.1.7 The requester shall be informed in writing whether access has been granted or denied. If, in addition, the requester requires the reasons for the decision in any other manner, he must state the manner, and the particulars so required.
 - 12.1.1.1.8 If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request orally.
 - 12.1.1.1.9 Where a requester has requested Personal Information from the Company, which is subsequently provided, the requester may request a correction of such Personal
-

Information if the information is inaccurate. Such a request shall be made to the IO of the Company, and all correct information must be provided along with the request to correct on the prescribed form, where applicable

12.1.1.1.10 Where the Company holds Personal Information in respect of any person, such person may object to the processing or further processing of Personal Information. Such objection shall be in writing and directed to the IO of the Company.

12.2 Fees:

12.2.1 A requester who seeks access to a record containing Personal Information about that requester is not required to pay the request fee. Every other requester, who is not a personal requester, must pay the required request fee:

12.2.2 The IO of the Company will notify the requester (other than a personal requester) by notice, requiring the requester to pay the prescribed fee (if any) before further processing the request.

12.2.3 **The requester must pay the prescribed fee before any further processing can take place.**

Description	Cost per A4-size page or part thereof/item	Number of pages/items	Total
The request fee payable by every other requester	N/A	N/A	R140.00
Photocopy / printed black & white copy of A4-size page	R2.00		
Printed copy of A4-size page	R2.00		
For a copy in a computer-readable form on: a) Flash drive – to be provided by requester b) Compact disc – (i) if provided by requester (ii) if provided to the requester	R40.00 (i) R40.00 (ii) R60.00		
For a transcription of visual images per A4-size page	Service to be outsourced. Will depend on quotation from Service provider.		
Copy of visual images.			
Transcription of an audio record, per A4-size page	R24.00		
Copy of an audio record.			

Description	Cost per A4-size page or part thereof/item	Number of pages/items	Total
(i) Flash Drive – to be provided by requester	R40.00		
(ii) Compact disc	R40.00		
– (i) if provided by requester			
(ii) If provided to the requester	R60.00		
To search for and prepare the record for disclosure for each hour or part of an hour, excluding the first hour, reasonably required for such search and preparation.	R145.00		
To not exceed a total cost of	R435.00		
A deposit if payable if search exceeds 6 hours	Amount of deposit (calculated on one third of total amount per request).	Hours of search	
Postage, email or any other electronic transfer	Actual costs if any		

The requester may lodge an application to the court against the tender or payment of the request fee.

11.2.3.1.1. After the IO of the Company has made a decision on the request, the requester must be notified in the required form.

11.2.3.1.2. If the request is granted then a further access fee must be paid for the search, reproduction, preparation and for any time that has exceeded the prescribed hours to search and prepare the record for disclosure.

12.3 Decision

12.3.1 The Company will, within 30 days of receipt of the request, decide whether to grant or decline the request and give notice with reasons (if required) to that effect.

12.3.2 The 30-day period within which the Company has to decide whether to grant or refuse the request, may be extended for a further period of not more than 30 days if the request is for a large number of information, or the request requires a search for information held at another office of the Company and the information cannot reasonably be obtained within the original 30-day period. The Company will notify the requester in writing should an extension be sought.

13. Grounds for Refusal of Access to Records

13.1 The IO of the Company may, in terms of the Act or any other Act or law, refuse access to certain records. The requester will be informed in writing of the reasons for the refusal. The IO of the Company may refuse access to certain records where an insufficient motivation is submitted by the requester or where:

13.1.1 The main grounds for the Company to refuse a request for information relates to the:

13.1.1.1 mandatory protection of the privacy of a third party who is a natural person, which would involve the unreasonable disclosure of personal information of that natural person,

13.1.1.2 mandatory protection of the commercial information of a third party, if the record contains:

13.1.1.2.1 trade secrets of that third party,

13.1.1.2.2 financial, commercial, scientific or technical information which disclosure could likely cause harm to the financial or commercial interests of that third party,

13.1.1.2.3 information disclosed in confidence by a third party to the Company, if the disclosure could put that third party at a disadvantage in negotiations or commercial competition,

13.1.2 intellectual, private and confidential property and interests of the Company, its staff members and customers/policyholders are concerned,

13.1.3 mandatory protection of confidential information of third parties if it is protected in terms of any agreement or law,

13.1.4 mandatory protection of the safety of individuals and the protection of property,

13.1.5 mandatory protection of records which would be regarded as privileged in legal proceedings,

13.1.6 the commercial activities of the Company, which may include:

13.1.6.1 trade secrets of the Company,

13.1.6.2 financial, commercial, scientific or technical information which disclosure could likely cause harm to the financial or commercial interests of the Company,

13.1.6.3 information which, if disclosed could put the Company at a disadvantage in negotiations or commercial competition, and

13.1.6.4 a computer program, system or application which is owned by the Company, and which is protected by copyright.

13.2 Requests for information that are clearly intended to circumvent the discovery phase in legal proceedings.

13.3 Requests for information that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources shall be refused.

13.4 If the request for access is refused, the requester may lodge an application with a court as stipulated in section 56 of the Act.

14. Remedies

14.1 Internal Remedies

14.1.1 The Company does not have internal appeal procedures. As such, the decision made by the Information Officer is final, and requesters will have to exercise such external remedies at their disposal if the request for information is refused, and the requester is not satisfied with the answer supplied by the Information Officer.

14.2 External Remedies

14.2.1 Subject to the provisions of the Act, a requester that is dissatisfied with an Information Officer's refusal to disclose information, may within 180 days of notification of the decision, lodge a complaint with the Information Regulator or apply to a Court for relief.

14.2.2 Likewise, a third party dissatisfied with an Information Officer's decision to grant a request for information, may within 180 days of notification of the decision, lodge a complaint with the Information Regulator or apply to a Court with appropriate jurisdiction for relief.

15. Updating of the Manual

15.1 The Information Officer of the Company will on a regular basis update this manual.

16. Availability of the manual

16.1 This manual is also available for inspection, during office hours, at the offices of Aurora Insurance Company free of charge.

16.2 To the information regulator upon request.

17. Adoption and Approval

17.1 This Policy has been formally adopted by the Board of Directors.
