

PROMOTION OF ACCESS TO INFORMATION ACT MANUAL

Prepared in terms of section 51 of the Promotion of Access to Information Act 2 of 2000, as amended

Private body	Ankerdata Hospitality Systems (Pty) Ltd
Registration number	2013/194081/07
Effective date	August 2026
Version	1.0

Public availability

This manual is made available on the Company website and at its principal place of business. A copy may also be requested from the Information Officer.

This manual should be reviewed periodically and updated when material changes occur.



CONTENTS

1. Introduction and purpose
 2. Company particulars and Information Officer
 3. Guide issued by the Information Regulator
 4. Records available without a formal PAIA request
 5. Records held in accordance with other legislation
 6. Categories of records held by the Company
 7. How to request access to a record
 8. Fees
 9. Decision, time periods and form of access
 10. Grounds for refusing access
 11. Remedies and complaints
 12. Processing of personal information under POPIA
 13. Security safeguards
 14. Availability and updating of this manual
- Annexure A - Request checklist

1. INTRODUCTION AND PURPOSE

Ankerdata Hospitality Systems (Pty) Ltd (the “Company”) is a private company operating in the hospitality technology and related services sector. This manual is prepared in terms of section 51 of the Promotion of Access to Information Act 2 of 2000 (“PAIA”), as amended, and also addresses the information required by the Protection of Personal Information Act 4 of 2013 (“POPIA”).

The purpose of this manual is to describe the records held by the Company, explain how a person may request access to those records, and set out the Company’s processing of personal information. Access is not automatic: a requester must comply with PAIA and, for records of a private body, must identify the right that the requested record is required to exercise or protect and explain why the record is necessary for that purpose.

Nothing in this manual creates a right of access greater than the rights provided by PAIA, POPIA or any other applicable law.

2. COMPANY PARTICULARS AND INFORMATION OFFICER

Item	Details
Registered name	Ankerdata Hospitality Systems (Pty) Ltd
Registration number	2013/194081/07



Principal place of business

Unit B, No. 12, N1 City Mews, 5 Manus Gerber Road,
Goodwood, 7760

Information Officer

Ian Lumsden, Managing Director

Telephone

+27 (0)21 001 8846

Email

info@ankerdata.co.za

Website

www.ankerdata.co.za

All PAIA requests and related correspondence should be marked for the attention of the Information Officer and submitted using the contact details above.



3. GUIDE ISSUED BY THE INFORMATION REGULATOR

The Information Regulator has published a guide explaining how to use PAIA. The guide and prescribed PAIA forms are available from the Information Regulator's website. A person may also request assistance or a copy of the guide from the Information Regulator.

Information Regulator	Contact details
Physical address	Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191
Postal address	P.O. Box 31533, Braamfontein, Johannesburg, 2017
Telephone	010 023 5200 / Toll-free 0800 017 160
General enquiries	enquiries@infoeregulator.org.za
PAIA complaints	PAIAComplaints@infoeregulator.org.za
Website	www.infoeregulator.org.za

4. RECORDS AVAILABLE WITHOUT A FORMAL PAIA REQUEST

The following records may, where applicable and lawfully publishable, be available without a formal PAIA request:

- Information published on the Company website, including general company and product information, contact details, notices, policies and website terms;
- Public marketing material, brochures, media releases and public product documentation;
- Vacancy advertisements and other publicly issued recruitment information;
- Records available through the Companies and Intellectual Property Commission or another public register; and
- Any category of records formally identified by the Company as automatically available under PAIA.

Availability does not require the Company to disclose confidential, privileged, security-sensitive or personal information. Records not publicly available must be requested in the manner described in this manual.

5. RECORDS HELD IN ACCORDANCE WITH OTHER LEGISLATION

The Company may hold records in accordance with legislation applicable to its operations, including the following, as amended from time to time:

- Basic Conditions of Employment Act 75 of 1997;
- Companies Act 71 of 2008;
- Compensation for Occupational Injuries and Diseases Act 130 of 1993;



- Consumer Protection Act 68 of 2008;
- Electronic Communications and Transactions Act 25 of 2002;
- Employment Equity Act 55 of 1998;
- Income Tax Act 58 of 1962 and Tax Administration Act 28 of 2011;
- Labour Relations Act 66 of 1995;
- Occupational Health and Safety Act 85 of 1993;
- Protection of Personal Information Act 4 of 2013;
- Skills Development Act 97 of 1998 and Skills Development Levies Act 9 of 1999;
- Unemployment Insurance Act 63 of 2001 and Unemployment Insurance Contributions Act 4 of 2002;
- Value-Added Tax Act 89 of 1991; and
- Any other sectoral, contractual, tax, employment, technology or commercial legislation applicable to the Company.

The inclusion of legislation in this list does not imply that every record is available under PAIA. Access remains subject to the Act and any confidentiality, privilege, privacy, retention or statutory restrictions.



6. CATEGORIES OF RECORDS HELD BY THE COMPANY

The Company may hold records in the following categories. The list is illustrative and a category may not exist in every instance.

Category	Examples of records
Corporate and governance	Memorandum of Incorporation; statutory registers; shareholder and director records; resolutions; meeting minutes; governance policies; company secretarial records.
Finance, tax and insurance	Budgets; accounting records; invoices; banking records; tax returns; audit and management accounts; insurance policies and claims; asset registers.
Human resources	Employee and contractor records; employment agreements; payroll; leave; performance; training; disciplinary and grievance records; health and safety records.
Customers and commercial operations	Customer agreements; proposals; orders; correspondence; implementation and support records; service reports; account and billing information; complaints.
Suppliers and service providers	Supplier agreements; quotations; procurement and due-diligence records; invoices; performance and correspondence.
Products, technology and information systems	Product documentation; software development records; system configurations; technical specifications; support logs; access and security logs; backup and continuity records.
Intellectual property	Trade marks; copyright material; software source and object code; designs; know-how; licence agreements; confidentiality agreements.
Legal and compliance	Contracts; legal opinions; litigation and dispute records; regulatory correspondence; compliance registers; risk assessments; policies and procedures.
Marketing and communications	Marketing plans; public relations material; website content; event records; mailing lists; sales and campaign records.
Personal information	Personal information relating to employees, applicants, customers, users, suppliers, directors, shareholders and other data subjects as described in section 12.

7. HOW TO REQUEST ACCESS TO A RECORD



A request must be made on the prescribed Form 2: Request for Access to Record, available from the Information Regulator's website. The completed form must be sent to the Information Officer using the details in section 2.

The requester must:

1. Provide sufficient particulars to enable the Company to identify the requester and the requested record;
2. Identify the form of access required and provide contact details for notices;
3. Identify the right the requester seeks to exercise or protect and explain why the requested record is required for that purpose;
4. If acting for another person, provide proof of the capacity or authority in which the request is made;
5. Provide any information reasonably required to locate the record and assess the request; and
6. Pay any prescribed request fee or access fee that is lawfully required.

A person who cannot complete the form because of illiteracy or disability may ask the Information Officer for reasonable assistance.



8. FEES

The fees payable for a PAIA request are prescribed by regulation and may change from time to time. The Company will notify a requester of any fee payable and the method of payment. Where permitted by PAIA, the Company may require payment of a request fee, a deposit and the applicable access or reproduction fees before processing or providing access.

A personal requester seeking access to a record containing that requester's own personal information is not required to pay the request fee, although prescribed reproduction or access costs may still apply where legally permitted.

The current prescribed fee schedule should be consulted on the Information Regulator's website when a request is submitted.

9. DECISION, TIME PERIODS AND FORM OF ACCESS

The Company will generally decide a request within 30 days after receipt of a valid request, unless PAIA permits an extension. The requester will be notified in writing of the decision and, where access is granted, of the applicable fees and manner of access. If a request is refused, the notice will state adequate reasons for refusal and explain the available remedies, subject to the limits imposed by law.

Access may be provided by inspection, a copy, an electronic record, a transcription, or another form permitted by PAIA. The requested form of access will be provided where reasonably possible and not detrimental to the record, unreasonably disruptive, or contrary to law.

Where only part of a record is protected from disclosure, the Company will consider whether the protected portion can reasonably be severed and access granted to the remainder.

10. GROUNDS FOR REFUSING ACCESS

The Company may or must refuse access where PAIA so provides. Grounds may include:

- Protection of the privacy of a third party who is a natural person;
- Protection of confidential commercial information of a third party or the Company;
- Protection of information supplied in confidence;
- Protection of the safety of individuals or the security of property, systems or methods;
- Protection of legally privileged records;
- Protection of research information;
- Records whose disclosure is prohibited by law, court order, contract or an enforceable duty of confidence;
- Requests that are manifestly frivolous or vexatious, or that would involve an unreasonable diversion of resources, where PAIA permits refusal; and
- Any other mandatory or discretionary ground set out in PAIA.

Despite a ground of refusal, PAIA may require disclosure where the statutory public-interest override applies.



11. REMEDIES AND COMPLAINTS

A private body does not have an internal appeal procedure under PAIA. A requester or third party dissatisfied with a decision, or with a failure to decide within the required period, may lodge a complaint with the Information Regulator using the prescribed Form 5, after giving the Company a reasonable opportunity to address the matter where required. A complainant may also approach a competent court for appropriate relief within the time periods prescribed by law.

Complaints to the Information Regulator may be sent to PAIAComplaints@inforegulator.org.za. Supporting documents should include the original request, the Company's response (if any), relevant correspondence and proof of authority where the complaint is made on behalf of another person.



12. PROCESSING OF PERSONAL INFORMATION UNDER POPIA

12.1 Purpose of processing

The Company processes personal information only for lawful and legitimate business purposes, including:

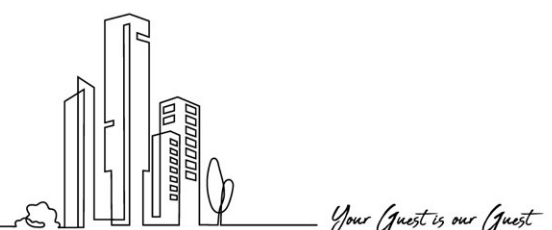
- Providing, implementing, supporting and improving hospitality technology products and services;
- Managing customer, user, supplier and business-partner relationships;
- Contract administration, billing, collections, accounting, tax and audit;
- Recruitment, employment, payroll, benefits, training and workforce management;
- Business communication, marketing and events, subject to applicable consent and opt-out requirements;
- Information security, access control, fraud prevention, incident management and business continuity;
- Compliance with legal, regulatory, contractual and governance obligations;
- Protecting and enforcing the Company's rights and resolving disputes; and
- Other compatible purposes permitted by law.

12.2 Categories of data subjects and personal information

Data subjects	Typical personal information
Employees, applicants and contractors	Identity and contact details; employment history; qualifications; payroll, tax and banking details; performance, leave and training information; limited health or special personal information where lawful and necessary.
Customers, users and prospective customers	Names, roles, contact details, account credentials, correspondence, service usage, support information, billing details and business relationship information.
Suppliers, advisers and business partners	Identity, contact, organisation, banking, tax, due-diligence, contractual and performance information.
Directors and shareholders	Identity and contact details; statutory, governance, shareholding, financial and compliance information.
Website visitors and communication recipients	Online identifiers, device and usage information, cookie data, enquiry details, communication preferences and marketing interaction data.
Other persons	Information contained in correspondence, complaints, legal matters, security records, visitor records or other legitimate business interactions.

12.3 Recipients or categories of recipients

Personal information may be shared, where lawful and necessary, with:



- Employees and authorised contractors who require access for their duties;
- Customers or business partners where necessary to deliver contracted services;
- Banks, payment providers, auditors, insurers, professional advisers and debt-recovery providers;
- Payroll, benefits, recruitment, cloud hosting, communications, security, software and other service providers;
- Regulators, revenue authorities, law-enforcement bodies, courts or other public authorities where required or permitted by law; and
- A purchaser, investor or adviser in connection with a lawful corporate transaction, subject to appropriate confidentiality and data-protection safeguards.

12.4 Cross-border transfers

The Company may use suppliers, systems or business partners located outside South Africa or may provide services across borders. Where personal information is transferred to another country, the Company will apply the requirements of section 72 of POPIA and use appropriate contractual, legal, consent-based or other safeguards as applicable.

12.5 Planned retention

Records are retained for periods determined by legal, regulatory, tax, employment, contractual, operational and legitimate business requirements. Records are securely deleted, destroyed or de-identified when they are no longer required, subject to lawful retention obligations and litigation holds.



13. SECURITY SAFEGUARDS

The Company uses reasonable and appropriate technical and organisational measures designed to protect personal information and other records against loss, damage, unauthorised destruction, unlawful access or unlawful processing. Measures may include:

- Role-based access controls, authentication and user-access management;
- Network, endpoint, application and cloud-security controls;
- Encryption or other protective measures where appropriate;
- Logging, monitoring, vulnerability management and incident-response processes;
- Backups, disaster recovery and business-continuity arrangements;
- Confidentiality obligations, policies, training and awareness;
- Supplier due diligence and data-protection provisions in contracts; and
- Secure retention, disposal and destruction procedures.

For security reasons, this manual does not disclose detailed technical configurations or controls. Security measures are reviewed and enhanced as risks, technologies and legal requirements evolve.

14. AVAILABILITY AND UPDATING OF THIS MANUAL

This manual is available:

- On the Company website at www.ankerdata.co.za;
- For inspection, by prior arrangement, at the Company's principal place of business during normal business hours; and
- On request from the Information Officer, subject to any lawful reproduction fee.

The Information Officer will review this manual periodically and update it when required by changes in law, Company operations, contact details or processing activities.

ANNEXURE A - REQUEST CHECKLIST

Before submitting a PAIA request to the Company, confirm that you have:

Check	Requirement
☐	Used the prescribed Form 2: Request for Access to Record.
☐	Clearly identified the record or category of records requested.
☐	Explained the right to be exercised or protected and why the record is required.
☐	Provided your identity and contact details.
☐	Selected the preferred form of access.
☐	Attached proof of authority if acting for another person.
☐	Sent the request to info@ankerdata.co.za for the attention of Ian Lumsden.
☐	Retained a copy of the request and proof of submission.



End of manual.

Ankerdata Hospitality Systems (Pty) Ltd.

Registration No: 1973/015515/07

Unit B, No. 12, N1 City Mews, 5 Manus Gerber Road, Goodwood, 7760

+27 (0)21 001 8846 • info@ankerdata.co.za • www.ankerdata.co.za



Your Guest is our Guest