

PAIA AND POPI MANUAL

Privacy is paramount

Published in terms of Section 51 of the Promotion of Access to Information Act 2 of 2000

This manual applies to

Konversant (Pty) Ltd

Registration number: [2013/192567/07] and all of its subsidiaries

(“**Organisation**”)

1. BACKGROUND TO THE PROMOTION OF ACCESS TO INFORMATION ACT

- 1.1 The Promotion of Access to Information Act, No.2 of 2000 (“**PAIA Act**”) was enacted on 3 February 2000, giving effect to the constitutional right in terms of section 32 of the Bill of Rights contained in the Constitution of the Republic of South Africa 108 of 1996 (the “**Constitution**”) of access to any information held by the state and any information that is held by another person that is required for the exercise or protection of any rights.
- 1.2 In terms of section 51 of the PAIA Act, all private bodies (juristic and natural persons) are required to compile an Information Manual (“**PAIA Manual**”).
- 1.3 Where a request is made in terms of the PAIA Act, the body to whom the request is made is obliged to release the information, subject to applicable legislative and/or regulatory requirements, except where the PAIA Act expressly provides that the information may be adopted when requesting information from a public or private body.

2. DETAILS OF ORGANISATION THIS MANUAL APPLIES TO

- 2.1 This manual was prepared in accordance with section 51 of the PAIA Act and to address requirements of the POPI Act for the Organisation.
- 2.2 The Organisation provides business consulting services with a focus on Human Capital Management and BBBEE consulting.
- 2.3 This PAIA manual is available at its premises: 5 Brackenhill Street, Boardwalk Meander, as well as on its website: www.konversant.co.za

3. PURPOSE

- 3.1 The purpose of the PAIA Act is to promote the right of access to information, to foster a culture of transparency and accountability within the Organisation by giving the right to information that is required for the exercise or protection of any right and to actively promote a society in which the people of South Africa have effective access to information to enable them to exercise and protect their rights.
- 3.2 In order to promote effective governance of private bodies, it is necessary to ensure that everyone is empowered and educated to understand their rights in relation to public and private bodies.
- 3.3 Section 9 of the PAIA Act recognizes that the right to access information cannot be unlimited and should be subjected to justifiable limitations, including, but not limited to:
 - 3.3.1 limitation aimed at the reasonable protection of privacy;
 - 3.3.2 commercial confidentiality;
 - 3.3.3 effective, efficient and good governance,

and in a manner which balances that right with any other rights, including such rights contained in the Bill of Rights in the Constitution.

- 3.4 This PAIA manual complies with the requirements of the guide contained in section 10 of the PAIA Act and recognizes that upon commencement of the POPI Act, that the appointed Information Regulator will be responsible to regulate compliance with the PAIA Act and its regulations by private and public bodies.

4. CONTACT DETAILS [Section 51(1)(a)]

- 4.1 The details of the Organisation that adopted this PAIA Manual is as follows:

Managing Director	Chrisna Strydom
Registered Address	5 Brackenhill Street, Boardwalk Meander
Postal Address	5 Brackenhill Street, Boardwalk Meander
Telephone Number	082 418 7575
Website	www.konversant.co.za

5. THE INFORMATION OFFICER [Section 51(1)(b)]

- 5.1 The PAIA Act prescribes the appointment of an Information Officer for the public bodies where such Information Officer is responsible to, inter alia, assess request for access to information.

- 5.2 The head of a private body fulfils such a function in terms of section 51 of the PAIA Act. The Organisation has opted to appoint the following person as Information Officer to assess such a request for access to information as well as to oversee its required functions in terms of the PAIA Act:

Information Officer	Chrisna Strydom
Physical address	5 Brackenhill Street, Boardwalk Meander
Telephone Number	082 418 7575
E-mail	chrisna@konversant.co.za

- 5.3 The Information Officer appointed in terms of the PAIA Act also refers to the Information Officer as referred to in the POPI Act. The Information Officer oversees the functions and responsibilities as required for in terms of both the PAIA Act as well as the duties and responsibilities in terms of section 55 of the POPI Act after registering with the Information Regulator.

5.4 The Information Officer may appoint, where it deemed necessary, Deputy Information Officers, as allowed in terms of section 17 of the PAIA Act as well as section 56 of the POPI Act. The Organisation has opted to appoint the following person as Deputy Information Officer to assist the Information Officer to assess such a request for access to information as well as to oversee its required functions in terms of the PAIA Act:

Deputy Information Officer	Stefmarie Lammerding
Physical address	5 Brackenhill Street, Boardwalk Meander
Telephone Number	082 323 1683
E-mail	admin@konversant.co.za

5.5 This is to render the Organisation as accessible as reasonable possible for requesters of its records and to ensure fulfilment of its obligations and responsibilities as prescribed in terms of section 55 of the POPI Act. All requests for information in terms of the PAIA Act must be addressed to the Information Officer.

6. **GUIDE OF SA HUMAN RIGHTS COMMISSION AND THE INFORMATION REGULATOR [Section 51(1)(b)]**

6.1 The PAIA Act grants a Requester access to records of a private body, if the record is required for the exercise to protection of any rights.

6.2 Requests in terms of the PAIA Act shall be made in accordance with the prescribed procedures, at the rates provided. The forms and tariff are dealt with in paragraphs 6 and 7 of the PAIA Act.

6.3 Requests are referred to the Guide in terms of section 10 of the PAIA Act which has been compiled by the South African Human Rights Commission (“**SAHRC**”), which will contain information for the purposes of exercising Constitutional Rights. *The Guide is available from the SAHRC.*

6.4 The contact details of the SAHRC are:

Contact Body	The South African Human Rights Commission
Physical Address	PAIA Unit 29 Princess of Wales Terrace Cnr York and Andrew Streets Parktown
Postal Address	Private Bag 2700 Houghton 2041
Telephone Number	+27 11 877 3600

E-mail	PAIA@sahrc.org.za
Website	www.sahrc.org.za

6.5 Sections 110 and 114(4) of the POPI Act states that the SAHRC will be replaced as the Regulator under the PAIA Act and will be replaced with the Information Regulator. The Information Officer will take over the PAIA functions from SAHRC on such date as agreed to between the parties. Until then requests to access records of a private body can be made to the SAHRC or to the Information Regulator as follows:

Contact Body	The Information Regulator (South Africa)
Physical Address	JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
Postal Address	P.O Box 31533, Braamfontein, Johannesburg, 2017
Telephone Number	+27 (0)12 406 4818
E-mail	inforeg@justice.gov.za
Website	www.justice.gov.za/inforeg

7. LATEST NOTICE IN TERMS OF SECTION 52(2) (IF ANY) [Section51(1)(c)]

No notice has been published on the categories of records that are automatically available without a person having to request access in terms of section 52(2) of the PAIA Act.

8. SUBJECTS AND CATEGORIES OF RECORDS AVAILABLE ONLY ON REQUEST TO ACCESS IN TERMS OF THE ACT [Section 51(1)(e)]

8.1 Records held by the Organisation

8.1.1 This clause serves as reference to the categories of information that the Organisation holds. The information is classified and grouped according to records relating to the following subjects and categories:

Subject	Category
Companies Act Records	All trust deeds Documents of Incorporation Index of names of Directors Memorandum of Incorporation Minutes of meetings of the board of directors Minutes of meetings of shareholders Proxy forms

	<p>Register of debenture-holders</p> <p>Register of directors 'shareholdings</p> <p>Share certificates</p> <p>Share Register and other statutory registers and/or records and/or documents</p> <p>Special resolutions/Resolutions passed at General and Class meetings</p> <p>Records relating to the appointment of:</p> <p>Auditors</p> <p>Directors</p> <p>Prescribed officers</p> <p>Public Officers</p> <p>Secretary</p>
Financial Records	<p>Accounting records</p> <p>Annual Financial Reports</p> <p>Annual Financial Statements</p> <p>Asset Registers</p> <p>Bank statement</p> <p>Banking details and bank accounts</p> <p>Banking records</p> <p>Debtors/Creditors statements and invoices;</p> <p>General ledgers and subsidiary ledgers</p> <p>General reconciliation</p> <p>Invoices</p> <p>Paid Cheques</p> <p>Policies and procedures</p> <p>Rental Agreements; and</p> <p>Tax returns</p>
Income Tax records	<p>PAYE Records</p> <p>Documents issued to employees for income tax purposes</p> <p>Records of payments made to SARS on behalf of employees</p> <p>All other statutory compliances:</p> <p>VAT</p> <p>Regional Services Levies</p> <p>Skills Development Levies</p> <p>UIF</p> <p>Workmen's Compensation</p>
Personal Documents and Records	<p>Accident books and records</p> <p>Address lists</p> <p>Disciplinary Code and Records</p> <p>Employee benefit arrangement rules and records</p> <p>Employment contracts</p> <p>Employment Equity Plans</p> <p>Forms and Applications</p> <p>Grievance procedure</p> <p>Leave records</p> <p>Medical Aid records</p> <p>Payroll Reports/ Wage registers</p>

	<ul style="list-style-type: none"> Pension Fund Records Safety, Health and Environmental records Salary records SETA records Standard letters and notices Training Manuals Training records Workplace and Union agreements and records
Procurement Department	<ul style="list-style-type: none"> Standard terms and Conditions for supply of services and products Contractor, client and supplier agreements Lists of suppliers, products, services and distribution Policies and Procedures
Sales Department	<ul style="list-style-type: none"> Customer details Credit application information Information and records provided by a third party
Marketing Department	<ul style="list-style-type: none"> Advertising and promotional material
Risk Management and Audit	<ul style="list-style-type: none"> Audit reports Risk management frameworks Risk Management plans
Safety, Health and Environment	<ul style="list-style-type: none"> Complete Safety, Health and Environmental Risk assessment Environmental Management Plans Inquiries, inspections, examinations by environmental authorities
IT Department	<ul style="list-style-type: none"> Computer/mobile device usage policy documentation Disaster recovery plans Hardware asset registers Information security policies/standard/procedures Information technology systems and user manuals Information usage policy documentation Project implementation plans Software licensing System documentation and manuals
Corporate Social Responsibility (CSR)	<ul style="list-style-type: none"> CSR schedule of projects/records of organizations that receive funding Reports, books, publications and general information related to CSR spend Records and contracts of agreement with funded organizations

8.2 Note that the accessibility of the records may be subject to the grounds of refusal set out in this PAIA Manual.

8.3 Amongst other, records deemed confidential on the part of a third party, will necessitate permission from the third party concerned, in addition to normal requirements, before the Organisation will consider access.

9. RECORDS AVAILABLE WITHOUT REQUEST TO ACCESS IN TERMS OF THE PAIA ACT

9.1 Records of a public nature, typically those disclosed on the Organisation website and in its various annual reports, may be accessed without the need to submit a formal application.

9.2 Other non-confidential records, such as statutory records maintained at Companies and Intellectual Property Commission, may also be accessed without the need to submit a formal application. However, please note that an appointment to view such records will still have to be made with the Information Officer.

10. DESCRIPTION OF RECORDS OF THE BODY WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION [Section 51(1)(d)]

10.1 Where applicable to its operations, the Organisation also retains records and documents in terms of the legislation below. Unless disclosure is prohibited in terms of legislation, regulations, contractual agreement or otherwise, records that are required to be made available in terms of these shall be made available for inspection by interested parties in terms of the requirements and conditions of the PAIA Act and the POPI Act or in terms of the below mentioned legislation and applicable internal policies, should such interested parties be entitled to such information.

10.2 A request to access must be done in accordance with the prescriptions of the PAIA Act.

10.3 The legislation applicable to the Organisation includes but may not be limited to the following:

- 10.3.1 Auditing Professions Act, No 26 of 2005;
- 10.3.2 Basic Conditions of Employment Act, No 75 of 1997;
- 10.3.3 Broad-Based Black Economic Empowerment Act, No 53 of 2003;
- 10.3.4 Business Act, No 71 of 1991;
- 10.3.5 Companies Act, No 71 of 2008;
- 10.3.6 Compensation for Occupational Injuries & Diseases Act, 130 of 1993;
- 10.3.7 Competition Act, No 71 of 2008;
- 10.3.8 Constitution of the Republic of South Africa 2008;
- 10.3.9 Copyright Act, No 98 of 1978;
- 10.3.10 Customs and Excise Act, 91 of 1964;
- 10.3.11 Electronic Communications Act, No 36 of 2005;
- 10.3.12 Electronic Communications and Transactions Act No 25 of 2002;
- 10.3.13 Employment Equity Act No 55 of 1998;
- 10.3.14 Financial Intelligence Centre Act, No 38 of 2001;

- 10.3.15 Identification Act, No 68 of 1997;
- 10.3.16 Income Tax Act, No 58 of 1962;
- 10.3.17 Intellectual Property Laws Amendment Act No 38 of 1997;
- 10.3.18 Labour Relations Act, No 66 of 1995;
- 10.3.19 Long Term Insurance Act, No 52 of 1998;
- 10.3.20 Occupational Health and Safety Act, No 85 of 1993;
- 10.3.21 Pension Funds Act, No 24 of 1956;
- 10.3.22 Prescription Act, No 68 of 1969;
- 10.3.23 Prevention of Organised Crime Act, No 121 of 1998;
- 10.3.24 Promotion of Access to Information Act, No. 2 of 2000;
- 10.3.25 Protection of Personal Information Act, No 4 of 2013;
- 10.3.26 Regulations of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002;
- 10.3.27 Revenue Laws Second Amendment Act No. 61 of 2008;
- 10.3.28 Skills Development Levies Act No. 9 of 1999;
- 10.3.29 Short-Terms Insurance Act No. 53 of 1998;
- 10.3.30 Trust Property Control Act 57 of 1988;
- 10.3.31 Unemployment Insurance Contributions Act 4 of 2002;
- 10.3.32 Unemployment Insurance Act no.30 of 1966; and
- 10.3.33 Value Added Tax Act 89 of 1991.

10.4 It is further recorded that the accessibility of documents and records may be subject to the grounds of refusal set out in this PAIA Manual.

11. **DETAIL TO FACILITATE A REQUEST FOR ACCESS TO A RECORD OF THE ORGANISATION** **[Section 51(1)(e)]**

11.1 The Requester, as defined in the PAIA Act, must comply with all the procedural requirements contained in the PAIA Act relating to the request for access to a record.

11.2 The Requester must complete the prescribed form and submit same as well as payment of a request fee and a deposit (if applicable) to the Information Officer or the Deputy Information Officer at the postal or physical address or electronic mail address as noted in clause 5 above.

11.3 *The form can be obtained from the Information Regulator's website www.justice.gov.za/inforeg (Form C – Request for access to record of Private Body).*

11.4 The prescribed form must be filled in with sufficient information to enable the Information Officer to identify:

- 11.4.1 the record or records requested; and
- 11.4.2 the identity of the requester.

11.5 The Requester should indicate which form of access is required and specify a postal address or fax number of the Requester in the Republic of South Africa.

- 11.6 The Requester must state that he/she requires the information in order to exercise or protect a right, and clearly state what the nature of the right is so to be exercised or protected. The Requester must clearly specify why the record is necessary to exercise or protect such a right (section 53(2)(d) of the PAIA Act).
- 11.7 The Organisation will process the request within 30 (thirty) days, unless the Requester has stated special reasons to the satisfaction of the Information Officer that circumstances dictate that the above time periods not be complied with.
- 11.8 The Requester shall be advised whether access is granted or denied in writing. If, in addition, the Requester requires the reasons for the decision in any other manner, the Requester will be obliged to state which manner and the particulars required.
- 11.9 If a request is made on behalf of another person, then the Requester must submit proof of the capacity in which the Requester is making the request to the reasonable satisfaction of the Information Officer (section 53(2)(f) of the PAIA Act).
- 11.10 If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request orally.
- 11.11 The Requester must pay the prescribed fee, before any further processing can take place.
- 11.12 All information as listed in this clause 11 herein should be provided and failing which the process will be delayed until the required information is provided. The prescribed time periods will not commence until the Requester has furnished all the necessary and required information. The Information Officer shall sever a record, if possible, and grant only access to that portion requested and which is not prohibited from being disclosed.

12. REFUSAL OF ACCESS TO RECORDS

12.1 Grounds to Refuse Access

- 12.1.1 A private body such as the Organisation is entitled to refuse a request for information.
- 12.1.2 The main grounds for the Organisation to refuse a request for information relates to the:
- 12.1.2.1 mandatory protection of the privacy of a third party who is a natural person or a deceased person (section 63) or a juristic person, as included in POPI Act, which would involve the unreasonable disclosure of personal information of that natural or juristic person;
- 12.1.2.2 mandatory protection of personal information and for disclosure of any personal information to, in addition to any other legislative, regulatory or contractual agreements, to comply with the provisions of the POPI Act;

- 12.1.2.3 mandatory protection of the commercial information of a third party (section 64 of the PAIA Act) if the record contains:
 - 12.1.2.3.1 trade secrets of the third party;
 - 12.1.2.3.2 financial, commercial, scientific or technical information which disclosure could likely cause harm to the financial or commercial interests of that third party; or
 - 12.1.2.3.3 information disclosed in confidence by a third party to the Organisation, if the disclosure could put that third party at a disadvantage in negotiations or commercial competition;
- 12.1.2.4 mandatory protection of confidential information of third parties (section 65 of the PAIA Act) if it is protected in terms of any agreement;
- 12.1.2.5 mandatory protection of the safety of individuals and the protection of property (section 66 of the PAIA Act);
- 12.1.2.6 mandatory protection of records which would be regarded as privileged in legal proceedings (section 67 of the PAIA Act);
- 12.1.2.7 the commercial activities (section 68 of the PAIA Act) of a private body, such as the Organisation, which may include:
 - 12.1.2.7.1 trade secrets of the Organisation;
 - 12.1.2.7.2 financial, commercial, scientific or technical information which disclosure could likely cause harm to the financial or commercial interests of the Organisation;
 - 12.1.2.7.3 information which, if disclosed could put the Organisation at a disadvantage in negotiations or commercial competition;
 - 12.1.2.7.4 a computer program which is owned by the Organisation, and which is protected by copyright; or
 - 12.1.2.7.5 the research information (section 69 of the PAIA Act) of the Organisation or a third party, if its disclosure would disclose the identity of the Organisation, the researcher or the subject matter of the research and would place the research at a serious disadvantage; or
- 12.1.2.8 requests for information that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources shall be refused.
- 12.1.3 All requests for information will be assessed on their own merits and in accordance with the applicable legal principles and legislation.
- 12.1.4 If a requested record cannot be found or if the record does not exist, the Information Officer shall, by way of an affidavit or affirmation, notify the Requester that it is not possible to give access to the requested record. Such a notice will be regarded as a decision to refuse a request for access to the record concerned for the purpose of the PAIA Act. If the record should later be found, the Requester shall be given access to the record in the manner stipulated by the Requester in the prescribed form, unless the Information Officer refuses access to such record.

13. REMEDIES AVAILABLE WHEN THE ORGANISATION REFUSES A REQUEST

13.1 Internal Remedies

13.1.1 The Organisation does not have internal appeal procedures. The decision made by the Information Officer is final.

13.1.2 Requesters will have to exercise such external remedies at their disposal if the request for information is refused and the Requestor is not satisfied with the answer supplied by the Information Officer.

13.2 External Remedies

13.2.1 A Requestor that is dissatisfied with the Information Officer's refusal to disclose information, may within 30 (thirty) days of notification of the decision, may apply to a Court for relief.

13.2.2 For purposes of the PAIA Act, the Courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another court of similar status and a Magistrate's Court designated by the Minister of Justice and Constitutional Development, and which is presided over by a designated Magistrate.

14. ACCESS TO RECORDS HELD BY THE ORGANISATION

14.1 **Prerequisites for Access by Personal/Other Requester**

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

14.1.2 A Requester is any person making a request for access to a record of the Organisation.

14.1.3 There are 2 (two) types of requesters:

14.1.3.1 Personal Requester

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

14.1.3.1.2 The Organisation will voluntarily provide the requested information, or give access to any record with regard to the requester's personal information. The prescribed fee for reproduction of the information requested will be charged.

14.1.3.2 Other Requester

14.1.3.2.1 This Requester (other than a personal requester) is entitled to request access to information on third parties.

14.1.3.2.2 In considering such a request, the Organisation will adhere to the provisions of the PAIA Act. Section 71 of the PAIA Act requires that the Information Officer take all reasonable steps to inform a third party to whom the requested record relates of the request, informing him/her that he/she may make a written or oral representation to the Information Officer why the request should be refused or, where required, give written consent for the disclosure of the Information.

14.2 The Organisation is not obliged to voluntarily grant access to such records. The Requester must fulfil the prerequisite requirements, in accordance with the requirements of the PAIA Act and as stipulated in Chapter 5: Part 3, including the payment of a request and access fee.

15. **PRESCRIBED FEES [Section 51(1)(f)]**

15.1 Fees Provided by the PAIA Act

15.1.1 The PAIA Act provides for 2 (two) types of fees, namely:

15.1.1.1 a request fee, which is a form of administration fee to be paid by all Requesters except personal requesters, before the request is considered and is not refundable; and

15.1.1.2 an access fee, which is paid by all Requesters in the event that a request for access is granted. This fee is inclusive of costs involved by the private body in obtaining and preparing a record for delivery to the Requester.

15.1.2 When the request is received by the Information Officer, such officer shall by notice require the Requester, other than a personal requester, to pay the prescribed request fee, before further processing of the request (section 54(1) of the PAIA Act).

15.1.3 If the search for the record has been made and the preparation of the record for disclosure, including arrangement to make it available in the requested form, requires more than the hours prescribed in the regulations for this purpose, the Information Officer shall notify the Requester to pay as a deposit the prescribed portion of the access fee which would be payable if the request is granted.

15.1.4 The Information Officer shall withhold a record until the Requester has paid the fees as indicated below.

15.1.5 A Requester whose request for access to a record has been granted, must pay an access fee that is calculated to include, where applicable, the request fee, the process fee for reproduction and for search and preparation, and for any time reasonably required in excess of the prescribed hours to search for and prepare the record for disclosure including making arrangements to make it available in the request form.

15.1.6 If a deposit has been paid in respect of a request for access, which is refused, then the Information Officer concerned must repay the deposit to the Requester.

16. **REPRODUCTION FEE**

16.1 Where the Organisation has voluntarily provided the Minister with a list of categories of records that will automatically be made available to any person requesting access thereto, the only charge that may be levied for obtaining such records, will be a fee for reproduction of the record in question, which will be as follows:

Reproduction of Information Fees	Fees to be Charged
Information in an A-4 size page photocopy or part thereof	R 1,10
A printed copy of an A4-size page or part thereof	R 0,75
A copy in computer-readable format, for example: Compact disc	R 70,00
A transcription of visual images, in an A4-size page or part thereof	R 40,00
A copy of visual images	R 60,00
A transcription of an audio record for an A4-size page or part thereof	R 20,00
A copy of an audio record	R 30,00

16.2 Request Fees

16.2.1 Where a Requester submits a request for access to information held by an institution on a person other than the Requester himself/herself, a request fee in the amount of R50,00 is payable up-front before the institution will further process the request received.

16.3 Access Fees

16.3.1 An access fee is payable in all instances where a request for access to information is granted, except in those instances where payment of an access fee is specially excluded in terms of the PAIA Act or an exclusion is determined by the Minister in terms of section 54(8) of the PAIA Act. The applicable access fees which will be payable are:

Access of Information Fees	Fees to be Charged
Information in an A4-size page photocopy or part thereof	R 1,10
A printed copy of an A4-size page or part thereof	R 0,75
A copy in computer-readable format, for example: USB Compact disc	R 7,50 R 70,00
A transcription of visual images, in an A4-size page or part thereof	R 40,00
A copy of visual images	R 60,00

A transcription of an audio record for an A4-size page or part thereof	R 20,00
A copy of an audio record *Per hour or part of an hour reasonably required for such search.	R 30,00*
Where a copy of a record need to be posted the actual postal fee is payable.	

16.4 Deposits

16.4.1 Where the institution receives a request for access to information held on a person other than the Requester himself/herself and the Information Officer upon receipt of the request is of the opinion that the preparation of the required record of disclosure will take more than 6 (six) hours, a deposit is payable by the Requester.

16.4.2 The amount of the deposit is equal to 1/3 (one third) of the amount of the applicable access fee.

16.5 Collection Fees

16.5.1 The initial "request fee" of R50,00 should be deposited into the bank account nominated by the Organisation and a copy of the deposit slip, application form and other correspondence / documents, forwarded to the Information Officer via fax/ email.

16.5.2 All fees are subject to change as allowed for in the PAIA Act and as a consequence such escalations may not always be immediately available at the time of the request being made.

16.5.3 Requesters shall be informed of any changes in the fees prior to making a payment.

17. **DECISION**

17.1 Time Allowed to Institution

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

17.1.2 The 30 (thirty) day period within which the Organisation has to decide whether to grant or refuse the request, may be extended for a further period of not more than (30) thirty 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 Organisation and the information cannot reasonably be obtained within the original 30 (thirty) day period.

17.1.3 The Organisation will notify the Requester in writing should an extension be sought.

18. PROTECTION OF PERSONAL INFORMATION THAT IS PROCESSED BY THE ORGANISATION

18.1 The POPI Act requires the Organisation to inform their clients as to the manner in which their Personal Information is used, disclosed and destroyed.

18.2 Chapter 3 of the POPI Act provides for the minimum Conditions for Lawful Processing of Personal Information by a Responsible Party. These conditions may not be derogated from unless specific exclusions apply as outlined in the POPI Act.

18.3 In this clause 18 words and phrases shall have the meanings assigned to them as in the POPI Act.

18.4 The Organisation needs Personal Information relating to both individual and juristic persons in order to carry out its business and organisational functions. The manner in which this information is Processed and the purpose for which it is Processed is determined by the Organisation. The Organisation is accordingly a Responsible Party for the purposes of the POPI Act and will ensure that the Personal Information of a Data Subject:

18.4.1 is processed lawfully, fairly and transparently. This includes the provision of appropriate information to Data Subjects when their data is collected by the Organisation, in the form of privacy or data collection notices. The Organisation must also have a legal basis (for example, consent) to process Personal Information;

18.4.2 is processed only for the purposes for which it was collected;

18.4.3 will not be processed for a secondary purpose unless that processing is compatible with the original purpose.

18.4.4 is adequate, relevant and not excessive for the purposes for which it was collected;

18.4.5 is accurate and kept up to date;

18.4.6 will not be kept for longer than necessary;

18.4.7 is processed in accordance with integrity and confidentiality principles. This includes physical and organisational measures to ensure that Personal Information, in both physical and electronic form, are subject to an appropriate level of security when stored, used and communicated by the Organisation, in order to protect against access and acquisition by unauthorised persons and accidental loss, destruction or damage;

18.4.8 is processed in accordance with the rights of Data Subjects, where applicable. Data Subjects have the right to:

18.4.8.1 be notified that their Personal Information is being collected by the Organisation. The Data Subject also has the right to be notified in the event of a data breach;

18.4.8.2 know whether the Organisation holds Personal Information about them, and to access that information. Any request for information must be handled in accordance with the provisions of this PAIA Manual;

18.4.8.3 request the correction or deletion of inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained personal information;

- 18.4.8.4 object to the Organisation's use of their Personal Information and request the deletion of such Personal Information (deletion would be subject to the Organisation's record keeping requirements);
- 18.4.8.5 object to the processing of Personal Information for purposes of direct marketing by means of unsolicited electronic communications; and
- 18.4.8.6 complain to the Information Regulator regarding an alleged infringement of any of the rights protected under the POPI Act and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

18.5 Purpose of the Processing of Personal Information by the Organisation

- 18.5.1 As outlined above, Personal Information may only be processed for a specific purpose. The purposes for which the Organisation processes or will process a client's Personal Information is to **analyze BBBEE, EE, WSP and HR related matters. The client's supplier's information for example race/gender/ownership/financials will be used for analysis of procurement and BBBEE overall scores. The Personal Information will also be used for disciplinary issues, contractual issues or establishment, mentoring and coaching where very personal information is gathered. Personal Information may also be used to be uploaded onto cloud storage services such as Dropbox.**

18.6 Categories of Data Subjects and Personal Information/Special Personal Information relating thereto

- 18.6.1 As per section 1 of the POPI Act, a Data Subject may either be a natural or a juristic person. Below are the various categories of Data Subjects that the Organisation Processes Personal Information on and the types of Personal Information relating thereto:
- Individual / Natural; and/or
 - Juristic

18.7 Recipients of Personal Information

- 18.7.1 The Organisation may provide a Data Subject's Personal Information to the following recipients:
- **Konversant related:** Chrisna Strydom, Stefmarie Lammerding, Jeanette Van Zyl, Nerina de Clerq.
 - **External:** BBBEE auditors, disciplinary chairperson's, legal advisors, training companies, cloud storage services such as Dropbox and Onedrive, external verification and accreditation bodies such as SANAS, training service providers, Enterprise & Development suppliers, Socio Economic Development related companies, Ownership and financial structuring suppliers and accountants.

18.8 Cross-border flows of Personal Information

- 18.8.1 Section 72 of the POPI Act provides that Personal Information may only be transferred out of the Republic of South Africa if the:

- 18.8.1.1 recipient country can offer such data an “adequate level” of protection. This means that its data privacy laws must be substantially similar to the Conditions for Lawful Processing as contained in the POPI Act; or
- 18.8.1.2 Data Subject consents to the transfer of their Personal Information; or
- 18.8.1.3 transfer is necessary for the performance of a contractual obligation between the Data Subject and the Responsible Party; or
- 18.8.1.4 transfer is necessary for the performance of a contractual obligation between the Responsible Party and a third party, in the interests of the Data Subject; or
- 18.8.1.5 the transfer is for the benefit of the Data Subject, and it is not reasonably practicable to obtain the consent of the Data Subject, and if it were, the Data Subject, would in all likelihood provide such consent.

18.8.2 The Organisation’s planned cross-border transfers of Personal Information and the condition that applies thereto is:

18.9 Description of information security measures to be implemented by the Organisation

18.9.1 The types of security measures to be implemented by the Organisation in order to ensure that Personal Information is respected and protected is:

- Anti-virus and password protected computers

18.9.2 A preliminary assessment of the suitability of the information security measures implemented or to be implemented by the Organisation may be conducted in order to ensure that the Personal Information that is processed by the Organisation is safeguarded and Processed in accordance with the Conditions for Lawful Processing.

18.10 Objection to the Processing of Personal Information by a Data Subject

18.10.1 Section 11 (3) of the POPI Act and regulation 2 of the POPI Act Regulations provides that a Data Subject may, at any time object to the Processing of his/her/its Personal Information in the prescribed form (Form 1 to be obtained under the POPI Act Regulations), subject to exceptions contained in the POPI Act.

18.11 Request for correction or deletion of Personal Information

18.11.1 Section 24 of the POPI Act and regulation 3 of the POPI Act Regulations provides that a Data Subject may in the prescribed form (Form 2 to be obtained under the POPI Act Regulations) request for their Personal Information to be corrected or deleted.

19. AVAILABILITY AND UPDATING OF THE PAIA MANUAL

19.1 This PAIA Manual is made available in terms of Regulation Number R.187 of 15 February 2002. The Organisation will update this PAIA Manual at such intervals as may be deemed necessary.

19.2 This PAIA Manual of the Organisation is available to view at its premises and on its website.

Document Owner:	Ink Legal (Pty) Ltd
Approved by:	Chrisna Strydom
Date approved:	June 2021
Due for review by Owner:	June 2022
Version:	1

POPI POLICY

Protection of Personal Information, Information Security and Records Management Policy

Privacy is paramount

This is the **Protection of Personal Information, Information Security and Records Management Policy** for

Konversant (Pty) Ltd

Registration Number: 2013/192567/07 and all its subsidiaries and divisions (hereinafter referred to as the “**the Organisation**”).

PROTECTION OF PERSONAL INFORMATION IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

1. INTRODUCTION

- 1.1 The Organisation is mainly a property management company that manages sectional title schemes and Homeowner Associations. This requires the Organisation to collect, collate, store and disseminate a vast amount of personal information on a daily basis, obliging the Organisation to comply with the Protection of Personal Information Act 4 of 2013 (“Act”).
- 1.2 The Act requires the Organisation to inform their clients as to the manner in which their personal information is used, disclosed and destroyed. The Organisation is committed to protecting its client’s privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.
- 1.3 This Policy sets out the manner in which the Organisation deals with their client’s personal information as well as stipulates the purpose for which said information is used.
- 1.4 The Policy is made available on the Organisation website www.konversant.co.za and by request from the Organisation.
- 1.5 The Policy is drafted in conjunction with the National Credit Act 34 of 2005, and the Consumer Protection Act 68 of 2008.

2. BACKGROUND AND PURPOSE

- 2.1 **What is the purpose of the Act (POPIA)?**
- 2.2 The aim of the Act is to ensure the right of South African citizens to the privacy of personal information and to regulate all organisations that collect, store and disseminate personal information.
- 2.3 Personal information may only be processed if the process meets the conditions of the Act.
- 2.4 There are **8 (eight) distinct conditions** which organisations need to meet to be acting lawfully:
- 2.4.1 **accountability;**
 - 2.4.2 **processing limitation;**
 - 2.4.3 **purpose specification;**
 - 2.4.4 **use limitation;**
 - 2.4.5 **information quality;**
 - 2.4.6 **openness;**
 - 2.4.7 **security safeguards; and**

2.4.8 **individual/data subject participation.**

2.5 **What is “personal information”?**

2.6 Personal information means any information relating to an identifiable natural person (and existing juristic persons where applicable), including information relating to:

2.6.1 race, gender, sex, pregnancy, marital status, mental health, well-being, disability, religion, belief, culture, language and birth;

2.6.2 education, medical, financial, criminal or employment;

2.6.3 identity number, electronic and physical addresses, telephone numbers and on-line identifiers;

2.6.4 biometric information;

2.6.5 personal opinions, views or preferences; and

2.6.6 correspondence sent by a person implicitly or explicitly of a personal nature or confidential.

2.7 An organisation may not process the personal information of a child (under 18) unless the processing:

2.7.1 is carried out with the consent of the legal guardian;

2.7.2 is necessary to establish, exercise or defence of a right or obligation in law;

2.7.3 is necessary for historical, statistical or research purposes; or

2.7.4 is information that is deliberately been made public by the child with the consent of the guardian.

2.8 **What is processing personal information?**

2.9 Processing means any operation or activity, or set of activities, by automatic means or otherwise, including:

2.9.1 collecting, receiving, recording, collating, storing, updating, modifying, retrieving or use;

2.9.2 disseminating by means of transmission, distribution or any other means; or

2.9.3 merging, linking, restricting, erasing or destructing of information.

2.10 **Who must comply?**

2.10.1 All public and private bodies (natural and juristic persons) must comply.

2.11 **What does compliance mean?**

2.11.1 Accountability

2.11.1.1 Organisations must assign responsibility to ensure compliance with the Act to a suitable person or persons.

- 2.11.1.2 Each organisation has an “**information officer**”. This will be the same person who has been appointed by the organisation as head in terms of the Promotion of Access to Information Act, i.e. the CEO or equivalent.
- 2.11.1.3 The information officer, together with an executive team/board, should decide on and record the POPI policy and procedure (this policy).
- 2.11.1.4 The information officer must appoint a “data controller” or a number of data controllers who decide:
 - 2.11.1.4.1 the purpose of the data processing; and
 - 2.11.1.4.2 the way the personal information should be processed.
- 2.11.1.5 The data controllers should be management who execute the POPI policy and procedure.
- 2.11.1.6 “Data processor/s” perform the processing administration/function (e.g. data capturing etc).
- 2.11.2 Processing limitation
 - 2.11.2.1 Personal information may only be processed if it is:
 - 2.11.2.1.1 adequate, relevant and necessary for the purpose for which it is processed;
 - 2.11.2.1.2 with the consent of the data subject;
 - 2.11.2.1.3 necessary for the contract to which the data subject is party;
 - 2.11.2.1.4 necessary for the protection of a legitimate interest of the data subject
 - 2.11.2.1.5 required by law;
 - 2.11.2.1.6 necessary to pursue the legitimate interest of the organisation; or
 - 2.11.2.1.7 collected directly from the data subject, except in certain circumstances (e.g. in public domain or to do so would defeat the purpose for collecting and processing).
 - 2.11.2.2 “**Consent**” must be:
 - 2.11.2.2.1 voluntary;
 - 2.11.2.2.2 specific; and
 - 2.11.2.2.3 informed.
 - 2.11.2.3 Informed consent requires that the data subject understand:
 - 2.11.2.3.1 what information is being collected/processed;
 - 2.11.2.3.2 why the information is being processed;
 - 2.11.2.3.3 how the information is to be processed;
 - 2.11.2.3.4 where the information is being processed; and
 - 2.11.2.3.5 to whom the information is intended to be given.
- 2.11.3 Purpose specification

2.11.3.1 The data subject must be made aware of the purpose for which the information is being collected (“identified purpose”). This is necessary for giving consent (see above).

2.11.4 Use limitation

2.11.4.1 Information/records may only be kept for as long as it is necessary to achieve the identified purpose. There are some statutory record keeping periods which may exceed this.

2.11.4.2 After this retention period the responsible person must delete or destroy such information as soon as reasonably possible.

2.11.4.3 If the purpose changes (e.g. something else occurs that could use the same information again for this alternative purpose), it may be necessary to inform the data subject and get consent again.

2.11.5 Information quality

2.11.5.1 Information must be as accurate as possible, complete and updated if necessary.

2.11.5.2 Information must be available to the data subject to verify/object to the accuracy thereof.

2.11.6 Openness

2.11.6.1 The Organisation must take reasonable practical steps to ensure that the data subject is aware of what personal information is being collected, stored and used, whether or not collected directly from the data subject.

2.11.7 Security safeguards

2.11.7.1 The organisation must secure the integrity and confidentiality of personal information and must take appropriate technical/organisational measure to prevent:

2.11.7.1.1 the loss of or damage to personal information; or

2.11.7.1.2 the unlawful access to or processing of personal information.

2.11.7.2 To do this, the organisation must:

2.11.7.2.1 identify all reasonable foreseeable internal and external risks to personal information held;

2.11.7.2.2 establish and maintain appropriate reasonable safeguards against the risks;

2.11.7.2.3 monitor the safeguards and regularly verify safeguards are effective; and

2.11.7.2.4 ensure safeguards are updated to respond to new risks or deficiencies in previous safeguards

2.11.7.3 The data controllers and data processors must operate under his/her authority from the information officer and treat all personal information as confidential.

2.11.7.4 Where there are reasonable grounds for suspecting a breach of data security, the responsible person must notify the Regulator and the data subject.

2.11.8 Data subject participation

2.11.8.1 Any person who can positively identify themselves is entitled to access their own personal information.

2.11.8.2 A data subject has the right to correct or amend any of their personal information that may be inaccurate, misleading or out of date.

2.12 **What steps should be taken to comply?**

2.12.1 An audit should be conducted of the following:

2.12.1.1 what personal information is held?

2.12.1.2 where the personal information is being held?

2.12.1.3 by whom is the personal information being held?

2.12.2 Establish what personal information is being collected in one place and being transferred to another.

2.12.3 Review website and other privacy statements, email indemnity, supplier or other standard terms and conditions, engagement letters, employee letters of appointment and third-party agreements that will process personal information of your clients or customers.

2.12.4 Develop organisation wide standard data protection policies and protocols, and if in place already in place, review such policies and protocols.

2.12.5 Review IT outsourcing contracts and arrangements.

2.12.6 Review data collecting activities (completion of forms etc).

2.12.7 Appoint an information officer for POPI and PAIA purposes.

2.12.8 Provide training to staff.

2.13 **Details of Information Officer and Head Office**

2.13.1 The details of the Organisation's Information Officer and Head Office are as follows:

Information Officer	Chrisna Strydom
----------------------------	-----------------

Physical address	5 Brackenhill Street, Boardwalk Meander
Telephone Number	082 418 7575
E-mail	chrisna@konversant.co.za

Deputy Information Officer	Stefmarie Lammerding
Physical address	5 Brackenhill Street, Boardwalk Meander
Telephone Number	082 323 1683
E-mail	admin@konversant.co.za

3 **PERSONAL INFORMATION COLLECTED**

- 3.1 Section 9 of the Act states that “**Personal Information**” may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not “**excessive.**”
- 3.2 The Organisation collects and processes client’s personal information to analyse BBBEE, EE, WSP and HR related matters. The client’s supplier’s information for example race/ gender/ ownership/ financials will be used for analysis of procurement and BBBEE overall scores. The Personal Information will also be used for disciplinary issues, contractual issues or establishment, mentoring and coaching where very personal information is gathered.
- 3.3 The type of information will depend on the need for which it is collected and will be processed for that purpose only.
- 3.4 Whenever possible, the Organisation will inform the client as to the information required and the information deemed optional.
- 3.5 The Organisation also collects and processes the client’s personal information for marketing purposes in order to ensure that our products and services remain relevant to our clients and potential clients.
- 3.6 The Organisation aims to have agreements in place with all product suppliers and third-party service providers to ensure a mutual understanding with regard to the protection of the client’s personal information. The Organisation suppliers will be subject to the same regulations as applicable to the Organisation.
- 3.7 With the client’s consent, the Organisation may also supplement the information provided with information the Organisation receives from other providers in order to offer a more

consistent and personalized experience in the client's interaction with the Organisation. For purposes of this Policy, clients include potential and existing clients.

4 THE USE OF PERSONAL INFORMATION

4.1 The Client's personal information will only be used for the purpose for which it was collected and as agreed. This may include:

- 4.1.1 providing products or services to clients and to carry out the transactions requested;
- 4.1.2 confirming, verifying and updating client details;
- 4.1.3 conducting market or customer satisfaction research;
- 4.1.4 for audit and record keeping purposes;
- 4.1.5 in connection with legal proceedings;
- 4.1.6 providing the Organisation services to clients, to render the services requested and to maintain and constantly improve the relationship;
- 4.1.7 providing communication in respect of the Organisation and regulatory matters that may affect clients;
- 4.1.8 in connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law; and
- 4.1.9 as required in terms of clause 3.2 above.

4.2 According to section 10 of the Act, personal information may only be processed if certain conditions, listed below, are met along with supporting information for the Organisation processing of Personal Information:

- 4.2.1 the client's consent to the processing: – consent is obtained from clients during the introductory, appointment and needs analysis stage of the relationship;
- 4.2.2 the necessity of processing: in order to conduct an accurate analysis of the client's needs;
- 4.2.3 processing complies with an obligation imposed by law on the Organisation;
- 4.2.4 the National Credit Act requires a Credit Provider's to conduct an affordability assessment
- 4.2.5 processing protects a legitimate interest of the client; or
- 4.2.6 processing is necessary for pursuing the legitimate interests of the Organisation or of a third party to whom information is supplied — in order to provide the Organisation clients with products and or services both the Organisation and any of our product suppliers require certain personal information from the clients in order to make an expert decision on the unique and specific product and or service required.

5 DISCLOSURE OF PERSONAL INFORMATION

5.1 The Organisation may disclose a client's personal information to any of the Organisation subsidiaries, joint venture companies and or approved product supplier or third-party service providers whose services or products clients elect to use. The Organisation has agreements in place to ensure compliance with confidentiality and privacy conditions.

- 5.2 The Organisation may also share client personal information with, and obtain information about clients from third parties for the reasons already discussed above.
- 5.3 The Organisation may also disclose a client's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect the Organisation rights.
- 5.4 All employees have a duty of confidentiality in relation to the Organisation and clients.
- 5.5 Information on clients: Our clients' right to confidentiality is protected in the Constitution and in terms of the Law. Information may be given to a third party if the client has consented in writing to that person receiving the information.
- 5.6 The Organisation views any contravention of this policy very seriously and employees who are guilty of contravening the policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.

6 SAFEGUARDING PERSONAL INFORMATION

- 6.1 It is a requirement of the Act to adequately protect personal information. The Organisation will continuously review its security controls and processes to ensure that personal information is properly safeguarded.
- 6.2 The Organisation Information Officer is responsible for the compliance of the conditions of the lawful processing of personal information and other provisions of the Act. The Information Officer will be assisted by Deputy Information Officer/s.
- 6.3 This policy has been put in place throughout the Organisation and training on this policy and the Act has already taken place and will continue to be conducted by the Organisation.
- 6.4 Each new employee will be required to sign an Employment Contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of the Act.
- 6.5 Every employee currently employed within the Organisation will be required to sign an addendum to their Employment Contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of the Act.
- 6.6 All the Organisation electronic files or data are backed and stored off site.
- 6.7 The Organisation product suppliers, insurers and other third-party service providers will be required to sign a service level agreement guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as needed.

7 **CORRECTION OF PERSONAL INFORMATION**

- 7.1 Clients have the right to access the personal information the Organisation holds about them. Clients also have the right to ask the Organisation to update, correct or delete their personal information on reasonable grounds. Once a client objects to the processing of their personal information, the Organisation may no longer process said personal information.
- 7.2 The Organisation will take all reasonable steps to confirm its clients' identity before providing details of their personal information or making changes to their personal information.

8 **AMENDMENTS TO THIS POLICY**

- 8.1 Amendments to, or a review of this Policy, will take place on an ad hoc basis or at least once a year.
- 8.2 Clients are advised to access the Organisation's website periodically to keep abreast of any changes. Where material changes take place, clients will be notified directly or changes will be stipulated on the Organisation website or on request from the registered office of the Organisation.

9 **ACCESS TO DOCUMENTS**

- 9.1 All company and client information must be dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances:
- 9.1.1 where disclosure is under compulsion of law;
 - 9.1.2 where there is a duty to the public to disclose;
 - 9.1.3 where the interests of the Organisation require disclosure; or
 - 9.1.4 where disclosure is made with the express or implied consent of the client.

10 **REQUESTS FOR THE ORGANISATION INFORMATION**

- 10.1 This is dealt with in terms of the Promotion of Access to Information Act, 2 of 2000 ("PAIA"), which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) that is required for the exercise or protection of rights. Private bodies, like the Organisation, must however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third party.
- 10.2 In terms hereof, requests must be made in writing on the prescribed form to the Information Officer in terms of PAIA. The requesting party has to state the reason for wanting the information and has to pay a prescribed fee.

10.3 The Organisation's manuals in terms of PAIA, which contains the prescribed forms and details of prescribed fees, is available on the intranet and the Organisation website www.konversant.co.za

10.4 Confidential company and/or business information of the Organisation may not be disclosed to third parties as this could constitute industrial espionage. The affairs of the Organisation must be kept strictly confidential at all times.

11 **RETENTION OF DOCUMENTS**

11.1 Hard Copy – The statutory periods for the retention of documents are as per the Law. These are available on request.

11.2 Electronic Storage – The internal procedure requires that electronic storage of information: important documents and information must be referred to and discussed with IT who will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with the departments concerned.

11.3 Scanned documents: If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee, including: employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years; must be retained for a period of 3 years after termination of employment.

11.4 Section 51 of the Electronic Communications Act No 25 of 2005 requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used.

11.5 It is also required that all personal information which has become obsolete must be destroyed.

12 **DESTRUCTION OF DOCUMENTS**

12.1 Documents may be destroyed after the termination of the retention period specified in terms of the Law. Registration will request departments to attend to the destruction of their documents and these requests shall be attended to as soon as possible.

12.2 Each department is responsible for attending to the destruction of its documents, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in

the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Organisation pending such return.

12.3 After completion of the process in clause 13.2 above, the General Manager of the department shall, in writing, authorise the removal and destruction of the documents in the authorisation document. These records will be retained by Registration.

12.4 The documents are then made available for collection by the removers of the Organisation's documents, who also ensure that the documents are shredded before disposal. This also helps to ensure confidentiality of information.

12.5 Documents may also be stored off-site, in storage facilities approved by the Organisation.

13 **CROSS-BORDER FLOWS OF PERSONAL INFORMATION**

13.1 Section 72 of the Act provides that Personal Information may only be transferred out of the Republic of South Africa if the:

13.1.1 recipient country can offer such data an "adequate level" of protection. This means that its data privacy laws must be substantially similar to the Conditions for Lawful Processing as contained in the Act; or

13.1.2 the client or customer consents to the transfer of their personal information; or

13.1.3 transfer is necessary for the performance of a contractual obligation between the client or customer and the Organisation; or

13.1.4 transfer is necessary for the performance of a contractual obligation between the Organisation and a third party, in the interests of the client or customer; or

13.1.5 the transfer is for the benefit of the client or customer, and it is not reasonably practicable to obtain the consent of the client or customer, and if it were, the client or customer, would in all likelihood provide such consent.

Document Owner:	Ink Legal (Pty) Ltd
Approved by:	Chrisna Strydom
Date approved:	June 2021
Due for review by Owner:	June 2022
Version:	1