PROMOTION OF ACCESS TO INFORMATION MANUAL

Spytek Surveillance

2004/034022/23

Prepared in terms of the requirements of the
PROMOTION OF ACCESS TO INFORMATION ACT
No. 2 of 2000

Date Compiled: 23 May 2022

1. INTRODUCTION

The Promotion of Access to Information Act 2 of 2000 ("PAIA" or "the Act") gives effect to the Constitutional right of access to any information held by the state and any information that is held by another person and that is required for the exercise or protection of any rights. The Protection of Personal Information Act 2013 has amended the PAIA and also requires from private bodies to disclose certain information through the relevant organisation's PAIA Manual.

Specifically, section 51(1) of the Act, read with the Protection of Personal Information Act of 2013, requires a private body to compile a manual that must contain information as specified and required by both PAIA and POPI. In addition, the PAIA manual must set out the formal procedure that a person must follow in order to request to view, update or delete personal information held by the private body.

In this context, a "private body" is defined as any natural person who carries or has carried on any trade, business or profession, but only in such capacity or any partnership which carries or has carried on any trade, business or profession or any former or existing juristic person (e.g. any company, close corporation or business trust).

This organisation falls within the definition of a "private body" and this Manual has been compiled in accordance with the said provisions and to fulfil the requirements of the Act.

In terms of the Act, where a request for information is made to a body, there is an obligation to provide the information, except where the Act expressly provides that the information may not be released. In this context, Section 9 of the Act recognises that access to information can be limited. In general the limitations relate to circumstances where such release would pose a threat to the protection of privacy, commercial confidentiality, and the exercising of efficient governance.

Accordingly, this manual provides a reference to the records held and the process that needs to be adopted to access such records.

All requests for access to information (other than information that is available to the public) must be addressed to the Head of the Business named in section 2 of this Manual.

2. BUSINESS AND CONTACT DETAILS

Name of Business:	Spytek Surveillance
Head of Business:	Ms Lelo Nzimande
Position:	Director
Postal Address:	1292 Heuwel Avenue,, Centurion, Tshwane, Gauteng, 0157
Physical Address:	1292 Heuwel Avenue, Centurion, Tshwane, Gauteng, 0157
Phone Number:	0113181318
Email Address:	lelo@spytek.co.za
Website:	www.spytek.co.za

3. SECTION 51(1) OF THE PROMOTION OF ACCESS TO INFORMATION ACT (THE ACT)

3.1 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 the public interest.

3.2 Requests in terms of the Act must be made in accordance with the prescribed procedures, at the rates provided. The forms and tariff are dealt with in regulations 6 and 7 of the Act.

3.3 Requesters are referred to the Guide which, in terms of Section 10 as amended, has been compiled by the Information Regulator established in terms of section 39 of the Protection of Personal Information Act, 2013, and which contains information for the purposes of exercising Constitutional Rights.

A "Request for a copy of the Guide (Form 1)" is available at:

https://www.justice.gov.za/inforeg/docs2-f.html

The Guide is also available at:

Address:	JD House, 27 Stiemens Street Braamfontein, Johannesburg, 2001
Postal Address:	P.O. Box 31533 Braamfontein, Johannesburg, 2017
Tel Number:	010 023 5200
Email Address:	PAIACompliance@infoRegulator.org.za

4. RECORDS AVAILABLE IN TERMS OF SECTION 52(2) OF THE ACT

Not applicable.

5. RECORDS THAT ARE HELD AT THE OFFICES OF THE BUSINESS

The following is a list of records that are held at the business's office:

Administration

- Attendance registers
- Correspondence
- Founding Documents
- Licences (categories)
- Minutes of Management Meetings
- Minutes of Staff Meetings
- Shareholder Register
- Statutory Returns

Human Resources

- Conditions of Service
- Employee Records
- Employment Contracts
- Employment Equity Records
- General Correspondence
- Industrial and Labour Relations Records
- Information relating to Health and Safety Regulations
- Pension and Provident Fund Records
- Performance Appraisals
- Personnel Guidelines, Policies and Procedures
- Remuneration Records and Policies
- Salary Surveys
- Salary Scale Surveys
- Skills Requirements
- Staff Recruitment Policies
- Statutory Records
- Training Records

Operations

- Brochures on Company Information
- Client and Customer Registry
- Contracts
- General Correspondence
- Information relating to Employee Sales Performance
- Information relating to Work-In-Progress
- Marketing and Future Strategies
- Marketing Records
- Production Records
- Sales Records
- Suppliers' Registry

Finances

- Annual Financial Statements
- Asset Register
- Banking Records
- Budgets
- Contracts
- Financial Transactions
- General Correspondence
- Insurance Information
- Internal Audit Records
- Management Accounts
- Purchase and Order Information
- Stock Records
- Tax Records (company and employee)

Information Technology

- IT Policies and Procedures
- Network Diagrams
- User Manuals

Statutory Records:
At present these include records (if any) held in terms of:

- Basic Conditions of Employment 75 of 1997
- Close Corporations Act 69 of 1984
- Companies Act 71 of 2008
- Consumer Protection Act 68 of 2008
- Employment Equity Act 55 of 1998
- Electronic Communications and Transactions Act 25 of 2002
- Income Tax Act 95 of 1967
- Occupational Health & Safety Act 85 of 1993
- National Credit Act 34 of 2005
- Trade Marks Act 194 of 1993
- Value Added Tax Act 89 of 1991

6. PROCESSING OF PERSONAL INFORMATION

Purpose of Processing

- Fulfilling statutory obligations in terms of applicable legislation
- Historical record keeping, research and recording statistics necessary for fulfilling our business objectives.
- Keeping of accounts and records
- Marketing and advertising
- Monitoring, maintaining and managing our contractual obligations to customers, clients, suppliers, service providers, employees, directors and other third parties
- Obtaining information necessary to provide contractually agreed services to customers and clients
- Resolving and tracking complaints
- Staff administration
- Verifying information provided to us

Categories of Data Subjects

- Clients and client's employees (inclusion of member records), representatives, agents, contractors and service providers
- Healthcare patients and healthcare providers associated with patients
- Our stakeholders
- Suppliers and service providers and their respective authorised employees, representatives, agents, contractors and service providers of such suppliers and service providers

Categories of Personal Information processed

Natural Persons

- Names
- Physical and postal addresses
- Date of birth
- ID number
- Tax related information
- Nationality
- Gender
- Confidential correspondence
- Email address
- Telephone number
- Online identifier or other particular assignment to the person

Juristic Persons

- Names of contact persons
- Name of Legal Entity
- Registration Number
- Physical and Postal address and contact details
- Financial information
- Founding documents
- Tax related information
- Authorised signatories, beneficiaries, ultimate beneficial owners
- BBBEE information

Categories of special information processed

- Racial / ethnic origin
- Offences / alleged offences
- Religious or other beliefs
- Physical / mental health details
- Criminal proceedings, outcomes & sentences

Possible Recipients of Personal Information

- Employees of the organisation
- Third party verification agencies and credit bureau

Trans-border / cross border flows of personal information

It may be required from time to time need to share personal information of data subjects with third parties in other countries. Any sharing of personal information of data subjects with third parties in other countries will be done only if the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection which effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person, as set out in the Protection of Personal Information Act and the data subject consents to the transfer.

Any such transfer will have to be shown to be necessary for the performance of a contract between the data subject and the recipient in question, or for the implementation of pre-contractual measures taken in response to the data subject's request.

General Description of Information Security Measures

Up to date technology is employed to ensure the confidentiality, integrity and availability of the Personal Information under our care.

Measures include:

- Acceptable usage of personal information
- Access control to personal information
- All third parties with whom any contract exists are required to ensure that appropriate security, privacy and confidentiality obligations are observed.
- Computer and network security including Firewalls, Virus protection software and updated protocols
- Governance and regulatory compliance
- Information security and HR policies including Bring Your Own Device (BYOD) policies
- Internal process to report security breach or anticipated security breach
- Investigating and reacting to security incidents
- Logical and physical access control
- Monitoring access and usage of private information
- Physical security

- Retention and disposal of information
- Secure communications
- Security in the outsourcing of any activities or functions through appropriate contracts
- Training of staff members

We continuously establish and maintain appropriate, reasonable technical and organisational measures to ensure that the integrity of the Personal Information which may be in our possession or under our control, is secure and that such information is protected against unauthorised or unlawful processing, accidental loss, destruction or damage, alteration or access by having regard to the requirements set forth in law, in industry practice and generally accepted information security practices and procedures applicable.

7. INFORMATION REQUEST PROCEDURE

- The requester must use the prescribed form to make the request for access to a record. The prescribed form is available from the Head of Business named in Section 2 above. The form is also available from the website of the Department of Justice and Constitutional Development at www.doj.gov.za

- The request must be made to the Head of Business named in Section 2 above. This request must be made to the address, fax number or electronic mail address of the business.
- The requester must provide sufficient detail on the request form to enable the Head of Business to identify the record and the requester. The requester should also indicate which form of access is required. The requester should also indicate if any other manner should be used to inform the requester. If this is the case, please furnish the necessary particulars to be so informed.

- The requester must identify the right that is sought to be exercised or to be protected and must provide an explanation of why the requested record is required for the exercise or protection of that right.

- If a request is made on behalf of another person, the requester must submit proof of the capacity in which the requester is making the request to the satisfaction of Head of Business aforesaid.

- The prescribed request fee must be attached.

- We will respond to your request within 30 days of receiving the request by indicating whether your request for access has been granted or denied.

- Please note that the successful completion and submission of a request for access form does not automatically allow the requestor access to the requested record.

Access will be granted to a record only if the following criteria are fulfilled:

- The record is required for the exercise or protection of any right; and

- The requestor complies with the procedural requirements set out in the Act relating to a request; and

- Access to the record is not refused in terms of any ground for refusal as contemplated in Chapter 4 of Part 3 of the Act.

8. DENIAL OF ACCESS

Access to any record may be refused under certain limited circumstances. These include:

- The protection of personal information from unreasonable disclosure concerning any natural person;
- The protection of commercial information held concerning any third party (for example trade secrets);
- The protection of financial, commercial, scientific or technical information that may harm the commercial or financial interests of any third party;
- Disclosures that would result in a breach of a duty of confidence owed to a third party;
- Disclosures that would jeopardize the safety or life of an individual;
- Disclosures that would prejudice or impair the security of property or means of transport;
- Disclosures that would prejudice or impair the protection of a person in accordance with a witness protection scheme;
- Disclosures that would prejudice or impair the protection of the safety of the public;
- Disclosures that are privileged from production in legal proceedings unless the privilege has been waived;
- Disclosures of details of any computer programme;
- Disclosures that will put Spytek Surveillance at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;
- Disclosures of any record containing any trade secrets, financial, commercial, scientific, or technical information that would harm the commercial or financial interests of Spytek Surveillance;
- Disclosures of any record containing information about research and development being carried out or about to be carried out by Spytek Surveillance;

If access to a record or any other relevant information is denied, our response will include:

- Adequate reasons for the refusal; and
- Notice that you may lodge an application with the court against the refusal and the procedure including details of the period for lodging the application.

9. FEES

The applicable fees are prescribed in terms of the Regulations promulgated under the Act.

There are two basic types of fees payable in terms of the Act.

Request Fee

The non-refundable request fee of R 50 (excluding VAT) is payable on submission of any request for access to any record. This does not apply if the request is for personal records of the requestor. No fee is payable in such circumstances.

Access Fee

The access fee is payable prior to being permitted access to the records in the required form. The applicable fees are prescribed in terms of Part III of Annexure A as identified in Government Notice Number 187, Regulation 11.

10. MANUAL AVAILABILITY

A copy of this Manual may be obtained from the Head of Business referred to in Section 2 hereof

Any transmission costs or postage required in respect of hard copies of the Manual, will be for the account of the requester.