ACTIVETRACK
MONITORING SOLUTIONS

Demonstrating our company's compliance with the provisions of the Protection of Personal Information Act, 4 of 2013 ("the POPI Act")

TABLE OF CONTENTS

CONSENT TO PROCESSING OF PERSONAL & SPECIAL PERSONAL INFOR-MATION FOR PURPOSES OF THE PROTECTION OF PERSONAL INFORMA-TION ACT, 4 OF 2013 (POPI ACT)

To be completed by each data subject entering Active Park.

To be completed by the individual attending at Active Park & providing this information.

1 Balilizeli Construction Trading & Projects (Pty) Ltd ("Balilizeli") is the owner of Active Park, and is the re sponsible party who will be processing my Personal Information.
I acknowledge I have read & understand this. Tick box: ☐

2 By attending at Active Park, I consent to Balilizeli processing the following categories of personal info rmation: name, biometric information, race, number plate, vehicle license disc, driver's license and/or ID where no driver's license can be produced ("Personal Information").
I confirm I have read, understood and agree to this. Tick box: ☐

3 I may contact Balilizeli at 7 Drome Road, Formain, Lyndhurst, Gauteng, 2090 or by telephone and email: 011 551 1687 & stephen@activetrack.co.za for further information regarding my rights as a data subject, or general information. Kindly ask for our Information Officer, Stephen Boulton.
I confirm I have read & understand this. Tick box: ☐

4 My Personal Information will be collected to (1) promote the safety and security of persons and property entering, exiting and/or located at Active Park; and (2) demonstrate the security solutions implemented at Active Park to potential clients where strict confidientialty agreements are concluded. Note that we will not use your driver's license or ID for demonstrations to potential clients.
I confirm I have read, understand & agree to this. Tick box: ☐

5 I understand that my Personal Information is supplied on a voluntary basis. I should alert Balilizeli staff if I do not wish to provide my Personal Information. Even if I withhold my consent to processing my Personal Information, I will still be granted access to Active Park.
I confirm that I have read, understand & agree to this. Tick box: ☐

I understand that my Personal Information will be processed lawfully, in a reasonable manner that does not infringe on my privacy, and will only be processed for the purposes mentioned above. When considering the processing purposes in the context of the high crime rate in South Africa and measures implemented by office parks similar to Active Park, as well as the need to generate new business, I agree that the processing purposes are adequate, relevant, and not excessive. Furthermore, I acknowledge that my Personal Information will not be retained for longer than is necessary to achieve the processing purposes. In addition, I understand that Balilizeli maintains reasonable security safeguards to ensure the integrity and confidentiality of my Personal Information, and to prevent loss of, damage to or unauthorised destruction of my Personal Information, and unlawful access to or processing of my Personal Information. In the unlikely event of a data breach, Balilizeli will notify me.
I confirm that I have read, understand & agree to this. Tick box: ☐

Kindly note that you have the right to access a record or description of personal information held by Balilizeli, as well as the right to object to the processing of personal information on reasonable grounds; just contact our Information Officer whose details appear above.

Name of individual providing consent:

Name of employer of individual:

Signature:

Date of signature:

If you have any queries, or wish to learn more about our data processing activities, kindly consult the Monitoring Terms displayed at the entrance to Active Park, or contact our Information Officer. Our Privacy Policy, Security Measures, and Manual are available at Active Park reception. Copies are available on request.

Monitoring Terms

Protection of Personal Information Act, 4 of 2013 (POPI Act)

Kindly take note that Balilizeli ("the Responsible Party") conducts CCTV surveillance at Active Park.

Activeye, new machine learning technology, has been integrated into the on-site CCTV. The technology uses unique software developed by a tenant of Balilizeli in which Balilizeli holds an interest and is the first of its kind worldwide.

Implemented for your safety and security, together with that of persons and property located at Active Park, Activeye allows for the automated detection of gender, race, age, emotionality and biometric information of all persons entering, exiting and present at Active Park. This involves the processing of special personal information and consent of data subjects is therefore required before the processing occurs. **Consent is voluntary.** If the data subject withholds his/or her consent, the personal information will not be processed.

Balilizeli takes your privacy seriously and is fully **compliant with the provisions of the POPI Act.** To this end, Balilizeli processes your personal information strictly in accordance with the eight conditions for lawful processing.

Your personal information will be processed in a reasonable manner that does not infringe on your privacy and will only be processed for the purposes of promoting the safety and security of the persons and property, entering, exiting and/or located at Active Park; and demonstrations of the security solutions to potential clients (where strict confidentiality agreements are concluded) from time-to-time. Since the abovementioned security solutions used by Balilizeli are commonplace at office parks similar to Active Park, and that Activeye needs to be taken to market, the processing is adequate, relevant, and not excessive. Furthermore, your information will not be retained for longer than is necessary to achieve the aforementioned purposes. For the avoidance of doubt, no data will be stored for a period longer than five (5) years. Balilizeli maintains reasonable security safeguards to ensure the integrity and confidentiality of personal information in its possession, and to prevent loss of, damage to or unauthorised destruction of personal information, and unlawful access to or processing of personal information. In the unlikely event of a data breach, Balilizeli will notify you.

Please bear in mind that you have the right to access a record or description of personal information held by Balilizeli; just contact our information officer. Details of the information officer are set out below.

Our information officer is Stephen Boulton, who can be reached at:

stephen@activetrack.co.za ● 011 551 1687 ● 7 Drome Road, Formain, Gauteng, 2090.

Copies of our Privacy Policy, Security Measures, and Manual are available at Active Park reception, and can be made available electronically on request.

DATA PROCESSING AGREEMENT

by and between

ACTIVE TRACK (PTY) LTD

(registration number 2013/229226/07)

("the Customer")

and

IRIS AI (PTY) LTD

(registration number 2018/597920/07)

("Iris AI")

DATA PROCESSING AGREEMENT TERMS

1 DEFINITIONS

"Active Track" means Active Track (Pty) Ltd, an entity registered in accordance with the company laws of South Africa, with registration number 2013/229226/07.

"**Agreement**" means the Data Processing Agreement between Iris AI and the Customer for the rendering of Services, the terms of which are set out herein.

"**Data subject**", "**operator**", "**personal information**", "**processing**", "**processor**" and "**responsible party**" have the same meanings as in the Data Protection Legislation.

"**Customer**" means Active Track.

"**Customer Personal information**" means personal information that is submitted to Iris AI by the Customer and processed by Iris AI for the purposes of rendering the Services.

"**Data Protection Legislation**" means the Protection of Personal Information Act, 4 of 2013 ("the POPI Act"), and all other applicable laws in relation to data protection and any update, amendment or replacement of same.

"**Services**" means the data processing services rendered by Iris AI for and on behalf of the Customer at the Customer's specific instance and request, in accordance with the terms specified herein.

2 DATA PROCESSING

2.1 Processing. In its processing of Customer Personal Information, Iris AI shall:

(a) comply in all material respects with applicable Data Protection Legislation; and

(b) implement appropriate technical, administrative, physical and organisational measures to adequately safeguard and protect the security and confidentiality of Customer Personal Information against accidental, unauthorized or unlawful destruction, alteration, modification, processing, disclosure, loss, or access.

2.2 Processing Instructions. The Customer instructs Iris AI to process Customer Personal Information for the following purposes:

(a) processing necessary for the provision of the Services;

(b) processing in accordance with Iris AI's privacy policy; and

(c) processing to comply with other reasonable instructions provided by the Customer to Iris AI (eg. via email) where such instructions are consistent with the terms of the Agreement.

2.3 Confidentiality: Iris AI will ensure that all Iris AI personnel involved in the processing of Customer Personal Information are party to confidentiality obligations in respect of the Customer Personal Information.

2.4 Assistance: Iris AI will (to the extent that it is reasonably able) provide any assistance reasonably required by the Customer where the Customer conducts a data protection impact assessment involving the Services and shall co-operate as reasonably requested by the Customer to enable the Customer to comply with any exercise of rights by a data subject under the Data Protection Legislation in re-

spect of Customer Personal Information. Any assistance provided by Iris AI under this section 2.4 shall be at the sole cost of the Customer.

2.5 Customer Processing. The Customer will, in its use of the Services, process Customer Personal Information in accordance with the requirements of Data Protection Legislation. The Customer's instructions to Iris AI for the processing of Customer Personal Information will comply with Data Protection Legislation and the Customer will have sole responsibility for the accuracy, quality, and legality of Customer Personal Information and the means by which the Customer acquired Customer Personal Information.

3 SUB-PROCESSORS

Sub-processing. Iris AI does not, and will not, engage the services of any sub-processors to process or sub-process Customer Personal Information in connection with the provision of the Services.

4 SECURITY

4.1 Security Measures. Iris AI implements the comprehensive administrative, technical, and physical safeguards contained in the Security Measures of Iris AI document, which appears at the end of this Agreement marked annexure "A", with respect to the Customer Personal Information. These security measures may be updated from time to time and Iris AI will notify the Customer where an update to these measures results in a material decrease in the levels of security applicable to Customer Personal Information

5 SECURITY INCIDENT NOTIFICATION

5.1 Security Incident. If Iris AI becomes aware of any unauthorized or unlawful access to, or acquisition, alteration, use, disclosure, or destruction of, Customer Data ("**Security Incident**"), it will take reasonable steps to notify the Customer without undue delay, but in any event within 72 hours of becoming aware of the Security Incident. Iris AI will also reasonably co-operate with the Customer with respect to any investigations relating to a Security Incident with preparing any required notices, and provide any information reasonably requested by the Customer in relation to any Security Incident.

6 AUDITS

6.1 Audit Procedures. The parties agree that audits will be carried out in accordance with the following conditions:

(a) The Customer will provide Iris AI with at least one (1) month's prior written notice of any audit by sending such notice to info@irisai.co.za, which may be conducted by the Customer or an independent auditor appointed by the Customer (provided that no person conducting the audit shall be, or shall act on behalf of, a competitor of Iris AI) ("Auditor");

(b) Iris AI agrees, subject to any appropriate and reasonable confidentiality restrictions, to provide evidence of any certifications and compliance standards it maintains and will, on request, make available to you an executive summary of Iris AI's most recent penetration tests, which summary shall include remedial actions taken by Iris AI resulting from such penetration tests.

(c) The scope of the certifications and penetration tests provided will be limited to Iris AI systems, processes, and documentation relevant to the processing and protection of personal data undertaken for the Services obtained by you, and the auditor will conduct audits subject to any appropriate and reasonable confidentiality restrictions requested by Iris AI.

(d) You will promptly notify and provide Iris AI with full details regarding any perceived non-compliance or security concerns discovered during the course of an audit.

6.2 The Customer may exercise the audit rights granted herein by instructing Iris AI to execute the audit

as described in this Section 6.

6.3 The parties agree that, except as otherwise required by a court order or other binding instruction of a regulator with authority over the Customer, this section 6 sets out the entire scope of the Customer's audit rights under.

7 TERMINATION & RETURN OF DATA

7.1 The term of this Agreement will terminate automatically on the later of: (i) the expiration or termination of the Agreement; or (ii) the deletion period referred to in clause 7.2 below.

7.2 Following termination of the Agreement, Iris AI shall, at the direction of the Customer return or delete all Customer Personal Information in accordance with the relevant provisions of the Agreement or, in the absence of any instruction from the Customer shall delete Customer Personal Information within 6 months unless, and to the extent only in each case, that legislation applicable to Iris AI requires further storage of the Customer Personal Information. Iris AI also retains the rights set out in the Agreement, to include the right to close and delete all data pertaining to a terminated Agreement on notice to the Customer.

8 GENERAL

8.1 Liability. Any and all claims brought under this Agreement whether in contract, delict (including negligence), for breach of statutory duty or otherwise howsoever arising will be subject to the same terms and conditions, including the exclusions and limitations of liability, as are set out in the Agreement.

8.2 Electronic Copy. This Agreement is delivered as an electronic document.

8.3 Entire Agreement. This Agreement constitutes the entire agreement between the parties and it supersedes any other prior or contemporaneous agreements or terms and conditions, written or oral, concerning its subject matter.

8.4 Severability. If any provision of this Agreement is determined to be unenforceable by a court of competent jurisdiction, that provision will be severed and the remainder of terms will remain in full effect.

8.5 Governing Law. This Agreement will be governed by the laws of South Africa. The High Court of South Africa, Gauteng Local Division, Johannesburg shall have non-exclusive jurisdiction over any dispute arising pursuant to this Agreement.

SIGNED AT ..... ON THIS ..... DAY OF .....

.....	.....
For and on behalf of the Customer, who warrants that he/or she is duly authorised to sign this Agreement.	For and on behalf of Iris AI, who warrants that he/or she is duly authorised to sign this Agreement.
Name:	Name: .....
Designation:	Designation: .....

Annexure "A"

Security Measures of Iris AI

Data and privacy organisation of Iris AI

The employees of Iris AI have specific roles that limit their access to business-critical information and personal information. Access management controls have been implemented according to the documented roles and responsibilities. The roles are listed below.

Sales & Support

Responsibilities:

- Customer acquisition
- Customer onboarding and setup
- Customer support (can also make changes according to customers' requests)
- Transfer bugs and technical support requests to developers

Access rights in Iris AI's products:

- Can see all organisations and edit their settings
- Can see and edit all the users and their access rights – all actions are logged
- Can't see customer's observations or audits
- Customer's observations and audits might be visible to the employee during onboarding, when the employee is part of the organisation in Iris AI's product.

Access to customer information outside Iris AI's products:

- Can have access to CRM and other marketing systems
    - These systems can contain personal data of prospects and other customer contact personnel.

Developers

Responsibilities:

- Product development (planning, coding, bug fixing & code reviews)
- Help support & sales with technical support requests

Access rights in Iris AI's products:

- Developers do not have access to production's servers and services.

Access outside Iris AI's products:

- Access to full application source code
- Access to error tracking system
    - The system can contain personal data that is used to identify who encountered the error
- Access to the staging environments of Iris AI products. The staging environments are completely isolated from production and do not contain any customer data.
- No access to production database, or backups
- No access to make code deployments to production environment
- No access to production application log systems

Core developers

Responsibilities:

In addition to the responsibilities listed under Developers:

- Manage code deployments
- Manage and support custom integrations
- Manage third party services used by the products which contain sensitive information (email sending, etc.)

Access rights in Iris AI's products:

- Same as developers

Access outside Iris AI's products:

In addition to the access listed under Developers:

- Full access to production databases
- Full access to database backups
- Full access to production application log systems
- Full access to third party services used by the service

Members:

Due to the access to business-critical and personal data, the Core Developer-role is granted to a limited group of people.

Marketing

Access rights in Iris AI's products:

- None

Access to customer information outside Iris AI's products:

- Can have access to CRM and other marketing systems
    - These systems can contain personal data of prospects and other customer contact personnel

Data and privacy matrix

	Sales & Support	Developers	Core Developers
View & edit organisation settings	✓	✓	✓
View & edit user access rights	✓	✓	✓
View observations or audits	✓*		
Source code		✓	✓
Error tracking		✓	✓
Application databases			✓
Application deployments			✓
Application log system			✓

** Can view during the onboarding phase.*

Iris AI security organisation

Name	Role	Responsibilities
Gerhard Furter	**Senior Engineer**	**Makes sure the development processes and software architecture adhere to the principles described within this document.**
Quintin Smith	**Core developer**	**Makes sure the development processes and software architecture adhere to the principles described within this document.**

Physical security of Iris AI premises

Access control

- The Iris AI premises is located within a secure office park. The server room is situated adjacent to the Iris AI premises. Access is restricted to the Iris AI premises, office park and server room.
- Employees gain access to the Iris AI premises via FPX10, a biometric fingerprint and RFID reader.[1] Access is restricted to business hours. Any work to be conducted outside business hours will be treated as an exception, and the restriction will be lifted for the particular period of work. Otherwise, the biometric reader denies access to the Iris AI employees after-hours.
- Access to the server room is similarly controlled via an FPX10 biometric fingerprint reader. Access is restricted to 4 employees. One can only gain access to the server room through the Iris AI premises. This adds an additional layer of security.
- All visitors to Iris AI premises and office park must be accompanied by Iris AI employees.
- Visitors are welcomed in a reception area and hosted in one of the company's boardrooms or auditoriums. These facilities are all located in the office park, in a building separate from the Iris AI premises.

Premises Protection & Physical Security

- The Iris AI premises is located within a secure office park. The office park is well-lit, has good visibility and is surrounded by a 2m security fence. Electric fencing is installed along the fence line and linked to an alarm. The alarm, in turn, is linked to a third party armed response company, National Security & Fire, formerly known as CHUBB Security.[2] CCTV is installed to monitor the fence line as an additional measure.
- Access is restricted to the Iris AI premises and office park itself.
- Access to and egress from the office park is controlled and recorded using a real-time access management system.
- Access to the Iris AI premises is denied outside of working hours.

1 https://activetrack.co.za/products/

2 National Security & Fire https://national.co.za

- Security officers of Maxi Security[3] are posted at the office park entrance. A security officer also carries out patrols along the perimeter of the office park.

- The security officer carries out his/her patrol with an Active Track device:[4] a hand-held guard monitoring device which tracks the movements of the officer in real-time. It also has panic buttons and distress signals that can be triggered if necessary. The Active Track devices are manufactured in Poland by EBS SP. z o.o.[5] and owned by entity Active Track[6] which is fully compliant with local privacy laws.

- CCTV is installed throughout the office park, as well as in the Iris AI premises and server room.

- A machine vision solution is integrated into the camera systems. The machine vision solution is provided by Activeye.[7] Activeye is fully compliant with local privacy legislation.

- The CCTV footage is managed and responded to by Maxi Security. Maxi Security's 24-hour control room is fully compliant with the standards prescribed by the South African Intruder Detection Services Association (SAIDSA).[8] Maxi Security complies with South Africa's privacy and security legislation, and by-laws.

- Doors to the Iris AI premises are self-closing and self-locking.

- The office park and Iris AI have appointed National Security & Fire as their armed response provider.

Security alarm system

- The physical alarm system is activated and deactivated manually by employees.

- The physical alarm system is tested regularly.

- Alarms generated pursuant to the Activeye-integrated CCTV are monitored in real-time by the Maxi Security 24-hour control room.

- A security officer on site is instructed by the control room operators to inspect any area on site where an alarm may be triggered.

- The officer will also be instructed to attend a particular area on site in real-time if Activeye determines that an unusual event may be taking place.

- The office park and Iris AI have appointed National Security & Fire as their armed response provider. National Security & Fire responds *inter alia* to fence alarms.

Fire Protection & Suppression

- The Iris AI premises is fitted with smoke alarms. Fire extinguishers are fitted in the Iris AI premises, and are serviced regularly by SANAS Accredited East Rand Fire.[9]

---

3 Maxi Phumelela Security (Pty) Ltd, a security services provider registered in accordance with the laws of South Africa with registration number 2001/001526/07. www.maxisecurity.co.za

4 https://activetrack.co.za/products/

5 EBS SP. Z O.O. https://www.ebssmart.com

6 Active Track (Pty) Ltd, with registration number 2013/229226/07. www.activetrack.co.za

7 Activeye Wireless (Pty) Ltd, a software development company incorporated in South Africa with registration number 2017/331604/07. www.activeye.co.za

8 http://www.saidsa.co.za/Bylaw6.pdf

9 East Rand Fire https://www.eastrandfire.co.za

- When it comes to the server room, it was designed in line with a professional fire risk assessment. Consequently, the following measures are in place:

    - A CO_2 Fire Detection & Suppression system has been installed, fitted with sirens and strobe lights which are activated in the event of an alarm condition.

    - Server room is kept clean and well-maintained, free of combustibles, as well as of dust and debris.

    - Two air conditioner units are installed which maintains a constant temperature of 18 degrees Celsius, keeping the equipment cool.

    - 24-hour monitoring of the server room by CCTV integrated with Activeye machine learning technology. An alarm will be triggered in the security control room if an abnormal behaviour is detected.

    - Internal and external inspections of fire protection measures. East Rand Fire routinely inspects our CO_2 Fire Detection & Suppression System.

    - Hands-on training of personnel, and regular fire drills.

Power

The Iris AI premises and server room electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours per day, seven days per week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. The server room uses generators to provide backup power for the entire facility.

Practical security matters at Iris AI

Password policy

- All Iris AI employees are required to use a password manager. Iris AI provides access to Steganos to all employees.
- Secure master password (at least 14 characters) should be used for accessing the password manager.
- The password manager should be used for generating a secure password for all applications and services.
- If some app has a default password it should be changed as soon as possible.

Connection security

- All Iris AI employees should always Iris AI main network inside Iris AI premises.
- Outside Iris AI premises employees should always use private networks or roaming instead of using public networks.

- Within Iris AI premises and the office park, visitors must always use the visitor network. In other words, the password of Iris AI network must never be exposed to anyone outside of the company.

Device security

Iris AI uses asset management to enforce device security. The asset management also includes an up-to-date inventory of device serial numbers. All devices used for work matters must be enrolled in the appropriate asset management system.

Laptop asset management

The laptop device security and asset management is managed through Steganos. The security policies in Steganos ensure that:

- Full disk encryption is enabled
- Password is required, and is at least 12 characters
- The laptop is locked after 3 minutes of inactivity
- Iris AI can remotely wipe the laptop

In addition, it is required that:

- All computers should be protected with appropriate Firewall software. Firewall

should always be updated to the newest version.

- Automatic software updates should always be installed as soon as possible.

Portable device asset management

Portable device security and asset management is managed through Silo. The asset management ensures that:

- Iris AI Silo Suite products cannot be accessed without accepting the security policies
- Device encryption is enabled
- Iris AI can remotely wipe the mobile device
- Device uses password - PIN code, or a fingerprint unlock

In addition, it is required that:

- All mobile devices must enter sleep mode after 30 seconds of leaving the device

unattended.

- Automatic software updates should always be installed as soon as possible.

Securely transferring information

Each employee is expected to handle sensitive, and business critical data with utmost care. This includes any information that a Customer sends in either physical or electronic format, or information that a Customer has provided to given contact person verbally. The following principles should apply:

- Employees do not store Customer information in their device hard-drives no longer than necessary.
- Any physical information provided by the Customer should be disposed of when it is no longer needed.
- Customer information within the applications should not be accessed unless absolutely necessary. Specific rules for accessing can be negotiated with the Customer.
- All Customer information should be stored within a single identifiable folder and the contents of this folder should be regularly checked for information that can be disposed of.
- Information and files containing sensitive, or business critical data should be shared between employees only when absolutely necessary. The information should be rather imported to the appropriate system right away, so that the safeguards of the target system will be enforced. If the information or file needs to be shared to an employee, it should be done through a safe channel, such as:
- Google Drive
- Gmail confidential email
- WhatsApp
- Unnecessary printouts of sensitive documents should be avoided. If a paper printout is necessary, it must be archived in a safe, or shredded as soon as possible.

Copies of production data

Sometimes it is necessary to test a certain feature or a fix for a bug with production data. The following principles should apply for testing:

- Features / bug fixes should only be tested with production data if absolutely necessary.
- If the feature / bug fix must be tested with production data, it should preferably be tested in a temporary testing server environment. Testing servers have the same security controls as the production server.
- Only if absolutely necessary should the developers take local copies of production data to their own working stations. In this case the production data should be immediately removed from the working station once the testing has been completed.

Memory sticks and portable storage devices

The use of memory sticks and other removable media is discouraged. The use of such devices for storing personally identifiable information is prohibited.

Policy violations

If any Iris AI employee violates the documented security policies, the following actions should take place:

- Director, and relevant manager, of Iris AI investigate what policy was violated and how serious the violation was.
- Director and relevant manager take the necessary actions with other executives of Iris AI.

Employee hiring and contract termination

- Each new employee gets introduced to the security matters at Iris AI.
- Each new employee that handles customer data signs a personal confidentiality and non-disclosure agreement.
- Customer can order background checks for Iris AI employees.
- Once an employee's contract is terminated, his or her access to all Iris AI services and applications is revoked.

Employee competency management

- Annual security training is mandatory for all employees
- Best practices are regularly and non-formally shared among teams
- Findings in external security audits are shared and discussed among the whole company

Risk management plan

Risk	Probability	Impact	Risk factor	Mitigation
Bankruptcy or other failure of main server provider	Very unlikely	Severe	Medium	Documented steps on how to install Iris AI applications to other cloud platforms.
Employee business continuity. For example, a key employee leaving Iris AI that has lots of tacit knowledge.	Possible	Moderate	Medium	Culture that endorses openness and sharing information. Making sure that in all business critical processes the bus factor is > 1.
The bankruptcy or other failure of other business critical SaaS providers.	Unlikely	Moderate	Medium	Iris AI has listed alternatives for all SaaS providers. Iris AI has changed many providers already while tendering their prices. Iris AI reviews yearly all its SaaS providers.
Hacked employee devices	Unlikely	Significant	Medium	Following industry best practices for securing employee devices. Using G Suite for centralized control of employee mobile devices.
Hacked servers	Very unlikely	Severe	Medium	Following best practices for password management. Choosing only the most trusted and best possible server providers.

Security by design

Software development processes

- Test driven development
- Automatic code coverage checks of unit tests
- Continuous integration
- Automatic code style checks
- Every change goes through extensive code review

Using open source libraries and components

Iris AI uses lots of open source in its applications. Each open source library and component gets reviewed before it is added to the application. The license of given library / component is also reviewed, so that it is compatible for commercial purposes.

Before updating any component, the changelog of given component is reviewed and checked.

Patch management

Microsoft Windows handles operating system updates and database security patches automatically.

Choosing SaaS partners

Iris AI uses only industry leading SaaS partners for providing its service. Each partner is carefully hand-picked, with special attention given on security. When selecting SaaS partner Iris AI checks the following things:

- What alternatives are there?
- How does the potential SaaS partner handle security?
- Size, revenue, ownership structure (if possible)

Annual security training

Iris AI offers annual security training to its employees. Attendance on these training sessions is mandatory and tracked.

Annual security audits

Iris AI conducts annual internal security audits that cover various aspects from physical security of our office premises, to security of our everyday processes.

Service security testing

Testing of security architecture is automated with comprehensive unit tests and continuous integration (CI). The CI server runs the tests after each commit in codebase. The unit tests are also run locally by the developers. On a typical day this means dozens of test runs.

Also, each line of code gets code reviewed by at least one developer before going to the production server.

Malware scanning

As an additional security measure PB services support malware scanning of attachments via Malware Bytes. Customers may choose whether or not they want to activate this option.

Compliance: GDPR & POPI Act

Iris AI ensures that all its applications are compliant with the provisions of both the GDPR and POPI Act. Iris AI ensures that all the server infrastructure and component providers are also GDPR and POPI Act compliant.

Iris AI maintains up-to-date documentation and practices regarding GDPR and the POPI Act in a workshop held every 6 months.

Data classification

While article 30 of the GDPR does not apply to Iris AI, the company maintains a data inventory for purposes of completeness. The Iris AI data inventory contains:

- The name of each controller on behalf of which Iris AI is acting
- The categories of processing carried out on behalf of each controller
- Confirmation that personal data is transferred to Iris AI in South Africa, and the Iris AI documentation specifying the suitable safeguards implemented
- A general description of the technical and organisational security measures referred to in Article 32(1) of the GDPR.

Data retention

General data deletion policy

Customer can issue deletion of specific database record or ask Iris AI to delete some range of records and their associated log entries. The records are permanently destroyed after one year, when the database backups containing those records are destroyed.

Customer specific data deletion policies

Iris AI allows customers to set their own data deletion policies. These policies can be set on user, observation category and observation question basis. The following use cases are possible:

- Setting the references for a given user role to be deleted from the system after a given time interval.
- Setting attachments for given concepts to be deleted from the system after a given time interval.

- Setting answers for given concepts to be deleted from the system after a given time interval.

Data retention after end of contract

Iris AI will retain the customer's data for 180 days after the end of contract. During this time period, the Customer can request a data handoff. After the 180 day time period Iris AI will remove the customer's data from all associated systems.

Data Protection Impact Assessments (DPIAs)

Iris AI assesses the need for a Data Protection Impact Assessment for a processing activity by referring to the GDPR Article 35:

> *Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.*

The need for a DPIA is assessed when the following activities occur:

- Implementation of integrations
- Customer onboarding projects that are different in terms of personal information handling from normal onboarding projects
- New features that involve processing activities of personal information
- When deciding to take a new data source

Existing DPIAs

Based on our assessment, Iris AI services do not have any processing activities that would fulfill the description of the GDPR article 35.

IT-security

Hardening

Iris Ai is operates as on a cloud application platform.

System Configuration:

System configuration and consistency is maintained through standard, up-to-date images, configuration management software, and by replacing systems with updated deployments. Systems are deployed using up-to-date images that are updated with configuration changes and security updates before deployment. Once deployed, existing systems are decommissioned and replaced with up-to-date systems.

Vulnerability Management

Our vulnerability management process is designed to remediate risks without customer interaction or impact. Iris AI is notified of vulnerabilities through internal and external assessments, system patch monitoring, and third party mailing lists and services. Each vulnerability is reviewed to determine if it is applicable to Iris AI's environment, ranked based on risk, and assigned to the appropriate team for resolution.

New systems are deployed with the latest updates, security fixes, and Iris AI configurations and existing systems are decommissioned as customers are migrated to the new instances. This process allows Iris AI to keep the environment up-to-date. Since customer applications run in isolated environments, they are unaffected by these core system updates.

To further mitigate risk, each component type is assigned to a unique network security group. These security groups are designed to only allow access to the ports and protocols required for the specific component type. For example, user applications running within an isolated dyno are denied access to the Iris AI management infrastructure as each is within its own network security group and access is not allowed between the two.

Application Security

We undergo penetration tests, vulnerability assessments, and source code reviews to assess the security of our application, architecture, and implementation. Our third party security assessments cover all areas of our platform including testing for OWASP Top 10 web application vulnerabilities and customer application isolation. Iris AI works closely with external security assessors to review the security of the Iris AI platform and applications and apply best practices.

Issues found in applications are risk ranked, prioritized, assigned to the responsible team for remediation, and Iris AI security team reviews each remediation plan to ensure proper resolution.

Network security

Iris AI ensures network security with firewalls, spoofing and sniffing protections, and by prohibiting port scanning.

The protection mechanisms are described below in more detail.

Firewalls

Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to only the ports and protocols required for a system's specific function to mitigate risk.

Host-based firewalls restrict customer applications from establishing localhost connections over the loopback network interface to further isolate customer applications. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.

Spoofing and Sniffing Protections

Managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the

hypervisor which will not deliver traffic to an interface which it is not addressed to. Iris AI utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels.

Port Scanning

Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.

Secure connections

All traffic between Customer and the cloud service is always transmitted over HTTPS. All connections are secured by either HTTPS or SSH.

Cryptography

The application uses PBKDF2-HMAC-SHA512 hashing algorithm for storing the hashes of users' passwords and authentication tokens.

The cloud service does not encrypt any data with public-key or symmetric-key algorithms.

SSL versions lower than 3.0 are prevented from accessing the service. At the moment the service supports encryption protocols TLS 1.2, TLS 1.1 and TLS 1.0. SSLv3 and SSLv2 are all supported. TLS 1.0 support will be removed by the end of 2020.

Data loss prevention

From Iris AI's security documentation:

> Continuous Protection keeps data safe on SQL Server 2019. Every change to your data is written to write-ahead logs, which are shipped to multi-datacenter, high-durability storage. In the unlikely event of unrecoverable hardware failure, these logs can be automatically 'replayed' to recover the database to within seconds of its last known state. We also provide you with the ability to backup your database to meet your own backup and data retention requirements.

Logging

Iris AI uses IIS Logs for searching and archiving logs. All HTTP requests, SQL queries taking longer than expected and executed worker tasks are logged.

The logged data for HTTP requests may include:

- user IP address
- time when the request was made
- execution duration
- size of the request content in bytes
- URL of the requested page

- HTTP status code of the response

For all HTTP POST requests an additional log entry is created that may contain:

- user ID (if user is logged in)
- all POST data excluding passwords and other sensitive information

Each database query taking longer than expected is logged with the following information:

- time when the query was executed
- query execution duration
- SQL statement

All errors are logged using Windows Event Logging. Each logged error contains the following information:

- time when the error occurred
- full error stack trace
- HTTP request details
- user who made the request (if any)
- IP address where the HTTP request originated from

The logs are archived for 1 year.

Windows Events error logging service does correlation analysis on logged error messages. It groups similar errors together and prioritizes the errors based on their occurrence.

All user activity which affects database is also stored in separate database version history. The version history can be used for checking which user was responsible for a certain change.

Log inspection and alerts

Iris AI has several alerts set up for our logs for certain unwanted scenarios. In some cases, these alerts also execute mitigating actions (for example, if a user has too many failed login attempts, the system will temporarily block succeeding attempts).

Availability

DDos attacks

The following quotation from Iris AI Security documentation describes how to mitigate DDoS attacks:

Our infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

In addition, Slowloris based DDoS attacks are mitigated with strict timeouts to keep connections open no longer than necessary and to reduce resource usage.

Disaster recovery plan (DRP)

> Our platform automatically restores customer applications and SQL databases in the case of an outage. The Iris AI platform is designed to dynamically deploy applications within the Iris AI cloud, monitor for failures, and recover failed platform components including customer applications and databases.

Backups

Automatic backups of the SQL databases are taken daily, weekly, and monthly. Daily backups are archived for one week, whereas weekly and monthly backups are archived for one month. Database backups will always be taken before deploying a new major version of the cloud service.

In addition to database backups, the cloud service keeps a version history for all successful database transactions.

Business continuity

Data centre failures

From Iris AI security documentation:

> The Iris AI platform is designed for stability, scaling, and inherently mitigates common issues that lead to outages while maintaining recovery capabilities. Our platform maintains redundancy to prevent single points of failure, is able to replace failed components, and utilizes multiple data centers designed for resiliency. In the case of an outage, the platform is deployed across multiple data centers using current system images and data is restored from backups. Iris AI reviews platform issues to understand the root cause, impact to customers, and improve the platform and processes.

Bankruptcy

It is possible to copy Customer owned information from the cloud database to Customer managed storage. This can be done manually by downloading a database dump of Customer's own data.

Physical security

The Hetzner facilities the cloud service uses adhere to ISO27001 and FISMA certificates.

Customer Applications and Databases

Our platform automatically restores customer applications and SQL Server databases in the case of an outage. The platform is designed to dynamically deploy applications within the Iris AI data center, monitor for failures, and recover failed platform components including customer applications and databases.

Iris AI Platform

The Iris AI platform is designed for stability, scaling, and inherently mitigates common issues that lead to outages while maintaining recovery capabilities. Our platform maintains redundancy to prevent single points of failure, is able to replace failed components, and utilizes multiple data centers designed for resiliency. In the case of an outage, the platform is deployed across multiple data centers using current system images and data is restored from backups. Iris AI reviews platform issues to understand the root cause, impact to customers, and improve the platform and processes.

Integrations

Iris AI offers various ways for integrating 3rd party software to its products.

SAML / ADFS integration

SAML / ADFS SSO integration is available for all of our products.

Data warehouse for BI tool integration

Iris AI may provide customers with credentials to a separate data warehouse database. The data in the warehouse database is updated once per day, and it can be analysed in the customer's own BI tool.

REST JSON API

All products have REST APIs. All the APIs are for our internal use only unless otherwise explicitly said, and they may change without any notice.

PB Gateway

PB Gateway is a separate service for updating user access rights based on user roles within a customer's own HR system. For large organisations PB Gateway can be essential for keeping access rights up-to-date.

Custom integrations

Iris AI has done various custom integrations in the past to different systems. These include integrations to property management systems, as well as SSO solutions.

Incident management

Customer notices serious security breach:

- The Customer contacts cyber security contact point either by email or by telephone.

- Iris AI incident management process.

Iris AI notices serious security breach:

- Iris AI informs the Customer.
- Iris AI incident management process.

Iris AI incident management process:

- Iris AI detects, records and classifies the incident.
- Iris AI gives initial support.
- Iris AI analyses the situation and either fixes the situation quickly or makes a proposal of possible mitigation procedures.
- Iris AI further analyses the incident and tries to think of possible scenarios of similar kind and how these could be mitigated as well.

Iris AI documents all security breaches and unplanned service disruptions.

References

- Iris AI https://irisai.co.za/
- National Security & Fire https://national.co.za
- Maxi Phumelela Security https://www.maxisecurity.co.za/
- Active Track products https://activetrack.co.za/products/
- EBS Poland https://www.ebssmart.com
- Activeye software development company http://activeye.co.za/
- SAIDSA by-laws http://www.saidsa.co.za/Bylaw6.pdf
- East Rand Fire https://www.eastrandfire.co.za/

Security Measures of Active Track

Pursuant to Condition 7: Security Safeguards of the POPI Act, 4 of 2013

	Category	Measure
1	**Physical Security**	All of Our Company's data processing equipment is hosted in the Iris AI data centre ("Data Centre") located in a secure office park. The office park can be found at 7 Drome Road, Formain, Lyndhurst, Gauteng, 2090. Access is restricted to both the office park and Data Centre by well-defined processes and ID Readers. They are also monitored on a 24/7 basis by security staff and surveillance cameras. A copy of the security measures implemented by Iris AI can be found on its website www.irisai.co.za. Alternatively, you can request a copy from our Information Officer.
2	**Logical access prevention**	Our Company's data processing systems are accessed by a limited number of authorised users with appropriate access rights. Dual-factor authentication is implemented for each role. Such access is restricted to a few users from the Administrative, Support and Management Teams. Within these teams, different roles are created based on the job requirements. Also, the activity of each user is monitored through monitoring solutions.
3	**Data access control**	Only a limited set of users from Our Company's Administrative, Support and Management Teams have access to the data processing systems which contain personal information. Data access privileges are defined by the job role of the user; accordingly, only authorised users with appropriate privileges have the access to personal information. No other user has any kind of access to this data. Our Company has implemented monitoring solutions to identify any attempts or actual unauthorised access to its systems and data.
4	**Data transfer control**	Our Company's processes and systems ensure that all personal information is encrypted whilst in transit or in storage. Our Company has implemented logging mechanisms to track data flows. Our Company's users have restricted access to personal information.
5	**Entry control**	Our Company has implemented logging and monitoring which enable tracking of changes and any addition/modification/deletion of personal information and by whom. Additionally, Our Company has implemented role-based access mechanisms along with dual-factor authentication.

6	**Instruction control**	Our Company has defined and implemented standard process and policies which require special approval of the concerned parties within its business, including operational, legal and technical teams. Pre-identified individuals from Our Company's Administrative and Support Teams are only involved in the actual processing of personal information. Pre-defined processes are in place to ensure that the confidentiality and the integrity of such data is maintained.
7	**Availability control**	Our Company has implemented well-defined disaster recovery plans which are tested on a regular basis. Back-up procedures and schedules have been defined and implemented.
8	**Separation control**	Data is separated both by logical and physical access controls. Network segmentations are in place to ensure that data is stored in the most restrictive zone of the network. Access to the data processing systems and the data itself is restricted by role-based privileges and dual-factor authentication. All access to the data systems and the data is logged and monitored. The production environment is completely segregated from the test environment.

Drafted and Published Pursuant to Section 17 of the Protection of Personal Information Act, 4 of 2013 read with Section 51 of the Promotion of Access to Information Act, 2 of 2000 (as amended)

1. INTERPRETATION

In this document, clause headings are for convenience and shall not be used in its interpretation unless the context clearly indicates a contrary intention:

1.1 an expression which denotes any gender includes the other genders; a natural person includes an artificial or juristic person and vice versa; the singular includes the plural and vice versa;

1.2 the following expressions shall bear the meanings assigned to them below and cognate expressions bear corresponding meanings:

1.2.1 "company" means Active Track (Pty) Ltd;

1.2.2 "this document" means this document together with any and all annexures, as amended from time to time;

1.2.3 "head of the company" means the information officer as defined in 1.2.4 below;

1.2.4 "information officer" means the person duly authorised by the head of the company and appointed by the company to facilitate or assist the head of the company with any request in terms of PAIA;

1.2.5 "PAIA" means the Promotion of Access to Information Act, 2 of 2000, as amended from time to time including the regulations promulgated in terms of PAIA;

1.2.6 "POPI Act" means the Protection of Personal Information Act, 4 of 2013, as amended from time to time include the regulations promulgated in terms of the POPI Act;

1.3 any reference to any statute, regulation or other legislation shall be a reference to that statute, regulation, or other legislation as at the signature date, and as amended or substituted from time to time;

1.4 if any provision in a definition is a substantive provision conferring a right or imposing an obligation on any party then, notwithstanding that it is only in a definition, effect shall be given to that provision as if it were a substantive provision in the body of this document;

1.5 where any term is defined within a particular clause other than this, that term shall bear the meaning ascribed to it in that clause wherever it is used in this document;

1.6 where any number of days is to be calculated from a particular day, such number shall be calculated as excluding such particular day and commencing on the next day. If the last day of such number so calculated falls on a day which is not a business day, the last day shall be deemed to be the next succeeding day which is a business day;

1.7 any reference to days (other than a reference to business days), months or years shall be a reference to calendar days, months, or years, as the case may be;

1.8 the use of the word "including" followed by a specific example/s shall not be construed as limiting the meaning of the general wording preceding it and the *eiusdem generis* rule shall not be applied in the interpretation of such general wording or such specific example/s;

1.9 insofar as there is a conflict in the interpretation of or application of this document and PAIA, PAIA shall prevail;

1.10 this document does not purport to be exhaustive of or comprehensively deal with every procedure provided for in the POPI Act or PAIA. A requester is advised to familiarise his/her/itself with the provisions of the POPI Act and PAIA before lodging any request with the company.

2. OBJECTIVE

To facilitate the requests for access to records of the company as provided for in the POPI Act and PAIA.

3. CONTACT DETAILS[1]

Company Registration No.:	2013/229226/07
Postal & Street Address:	7 Drome Road, Formain, Gauteng, 2090
Telephone Number:	011 551 1687
Fax Number:	086 537 6277
Website:	www.activetrack.co.za
Email:	info@activetrack.co.za
Information Officer:	Stephen Boulton
Email address:	stephen@activetrack.co.za
Telephone Number:	073 452 2987

4. THE GUIDE PRESCRIBED BY SECTION 10 OF PAIA[2]

4.1 Description

Pursuant to section 10 of PAIA, the South African Human Rights Commission has published the guide as is prescribed by section 10 of PAIA. The guide contains the necessary information to assist anyone who wishes to exercise any right under PAIA.

4.2 How to Access the Guide

The guide is available at the offices of the South African Human Rights Commission.[3]

The PAIA Unit at the South African Human Rights Commission

The Research & Documentation Department

Private Bag X2700

Houghton

2014

Telephone Number: 011 877 3600

Website: www.sahrc.org.za

Email: PAIA@sahrc.org.za

1 Section 51(1)(a)(i) of PAIA.

2 Section 51(1)(b)(i) of PAIA.

3 https://www.justice.gov.za/paia/dojcd-paia-manual.pdf

5. RECORDS HELD BY THE COMPANY IN TERMS OF OTHER LEGISLATION[4]

5.1 The following records are not automatically available without a request in terms of PAIA:

5.1.1 all statutory returns, namely VAT, workmen's compensation, UIF; regional services levies; and skills development levies.

5.1.2 documents concerning compliance by the company, insofar as it may be necessary, with legal obligations in terms of the Occupational Health and Safety Act, 85 of 1993 and any other applicable environmental legislation.

6. RECORDS THAT ARE AUTOMATICALLY AVAILABLE TO EITHER EMPLOYEES ONLY OR THE GENERAL PUBLIC AND EMPLOYEES[5]

6.1 The following records are automatically available to all employees of the company and need not be requested in accordance with the procedure outlined in paragraph 8 below:

6.1.1 personnel records are available to the employee whose file it is;

6.1.2 records of disciplinary hearings and related matters are available to the employee concerned;

6.1.3 the company's policies and procedures manual;

6.1.4 the company's document format manual.

6.2 The following records are automatically available to the general public and all employees and need not be requested in accordance with the procedure outlined in paragraph 8 below:

6.2.1 the company's employment equity plan;

6.2.2 the company's skills development plan.

7. OTHER TYPES OF RECORDS HELD BY THE COMPANY

These records are not automatically available without a request in terms of PAIA. A request in terms of this section is subject to section 63(1) of PAIA, which provides that the head of a company must refuse a request for access to a record of the company if the disclosure of the record would involve the unreasonable disclosure of personal information about a third party including a deceased individual.

7.1 Human Resources department

7.1.1 Personnel information, together with information on potential candidates, including personal information, employment history and health records that the company may hold from time to time.

7.1.2 Training and development information.

7.1.3 General files containing information on employee benefits and employee recruitment and selection information.

7.2 Project management

7.2.1 Building plans.

7.2.2 Information generally related to projects conducted by the company from time to time.

7.3 Information technology

7.3.1 Usage statistics

7.3.2 Equipment details

4 Section 51(1)(b)(iii) of PAIA.
5 Section 51(1)(b)(ii) of PAIA.

7.3.3 Costings of hardware and software

7.4 Catering

7.4.1 Function records and related costings

7.4.2 Stock sheets

7.4.3 List of suppliers

7.5 Companies department

Company secretarial records

7.6 Finance/Accounts department

7.6.1 Financial records

7.6.2 A list of the company's creditors and debtors

7.6.3 Salary information

7.6.4 Bank account information

7.6.5 Fixed assets register

7.7 Marketing department

7.7.1 Company brochures and publications

7.7.2 Documents relating to public relation events

7.7.3 Company media releases

7.8 Support services

7.8.1 Delivery and collection sheets

7.8.2 List of suppliers

7.8.3 Data relating to security measures in place

8. PROCESS OF REQUESTING INFORMATION NOT AUTOMATICALLY AVAILABLE

8.1 A request shall be made on the prescribed form. The form is downloadable at the following link: https://www.justice.gov.za/forms/paia/J752_paia_Form%20C.pdf The form is also available on the websites of the South African Human Rights Commissioner, and that of the Department of Justice and Constitutional Development.

8.2 The prescribed form shall be submitted to the information officer at her address, telefax number or e-mail address.

8.3 The same procedure as set out in 8.1 and 8.2 applies if the requester is requesting information on behalf of another person or on behalf of a permanent employee of the company.

8.4 The information officer, as soon as reasonably possible and within thirty days after the request has been received, shall decide whether or not to grant the request.

8.5 The requester will be notified of the decision of the information officer in the manner indicated by the requester.

8.6 If the request is granted, the requester shall be informed by the information officer in the manner indicated by the requester in the prescribed form.

8.7 Notwithstanding the aforegoing, the company will advise the requester in the manner stipulated by

the requester in the prescribed form of:

8.7.1 the access fee to be paid for the information (in accordance with paragraph 9);

8.7.2 the format in which access will be given; and

8.7.3 the fact that the requester may lodge an appeal with a court of competent jurisdiction against the access fee charged or the format in which access is to be granted.

8.8 After access is granted, actual access to the record requested will be given as soon as reasonably possible.

8.9 If the request for access is refused, the head of the company shall advise the requester in writing of the refusal. The notice of refusal shall state:

8.9.1 adequate reasons for the refusal;

8.9.2 that the requester may lodge an appeal with a court of competent jurisdiction against the refusal of the request (including the period) for lodging such an appeal.

8.10 Upon the refusal by the head of the company, the deposit paid by the requester will be refunded.

8.11 If the information officer fails to respond within thirty days after a request has been received, it is deemed, in terms of section 58 read together with section 56(1) of PAIA, that the head of the company has refused the request.

8.12 The head of the company may decide to extend the period of thirty days ("original period") for another period of not more than thirty days if:

8.12.1 the request is for a large number of records;

8.12.2 the search for the records is to be conducted at premises not situated in the same town or city as the head office of the company;

8.12.3 consultation among divisions or departments, as the case may be, of the company is required;

8.12.4 the requester consents to such an extension in writing; and

8.12.5 the parties agree in any other manner to such an extension.

8.13 Should the company require an extension of time, the requester shall be informed in the manner stipulated in the prescribed form of the reasons for the extension.

8.14 The requester may lodge an appeal with a court of competent jurisdiction against any extension or against any procedure set out in this section.

9. FEES PAYABLE

9.1 The fees for reproduction of a record as referred to in section 52(3) are as follows:

9.1.1 for every photocopy of an A4 size page or part thereof R 1.10

9.1.2 for every printed copy of an A4-size page or part thereof R 0.75

9.1.3 for a copy of a compact disc R 70.00

9.1.4 for a transcript of visual images for an A4 size page or part thereof R 40.00

9.1.5 for a copy of visual images R 60.00

9.1.6 for a transcript of an audio record, for an A4-size page or part thereof R 20.00

9.1.7 for a copy of an audio record R 30.00

9.2 The request fee payable by a requester, other than a personal requester, is R 50.00

9.3 If the head of the company is of the opinion that six hours will be exceeded to search, reproduce and/

or prepare the information requested, an upfront deposit is payable equal to R 30.00 for each hour or part thereof, exceeding the six hours.

10. INFORMATION OR RECORDS NOT FOUND

10.1 If all reasonable steps have been taken to find a record, and such a record cannot be found or if the records do not exist, then the head of the company shall notify the requester, by way of an affidavit or affirmation, that it is not possible to give access to the requested record.

10.2 The affidavit or affirmation shall provide a full account of all the steps taken to find the record or to determine the existence thereof, including details of all communications by the head of the company with every person who conducted the search.

10.3 The notice, as set out above, shall be regarded as a decision to refuse a request for access to the record concerned for the purposes of PAIA.

10.4 If the record in question 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 access is refused by the head of the company.

10.5 The attention of the requester is drawn to the provisions of Chapter 4 of Part 3 of PAIA in terms of which the company may refuse, on certain specified grounds, to provide information to a requester.

11. INFORMATION REQUESTED ABOUT A THIRD PARTY

11.1 Section 71 of PAIA makes provision for a request for information or records about a third party.

11.2 In considering such a request, the company will adhere to the provisions of sections 71 to 73 of PAIA.

11.3 The attention of the requester is drawn to the provisions of Chapter 5 of Part 3 of PAIA in terms of which the company is obliged, in certain circumstances, to advise third parties of requests lodged in respect of information applicable to or concerning such third parties. In addition, the provisions of Chapter 2 of Part 4 of PAIA entitle third parties to dispute the decisions of the head of the company by referring the matter to court.

12. ADDITIONAL INFORMATION PURSUANT TO THE POPI ACT

12.1 Section 52 of POPIA has been amended to include certain information in this manual, pursuant to the POPI Act coming into operation. Before the purpose of the processing is addressed, it must be mentioned that the company:

12.2.1 uses personal data from you when you visit the company website, make use of the company's services, or are employed by the company. To learn more about this, please read the privacy policy published on the company website www.irisai.co.za

12.2.2 the company processes the following information about you:

12.2.2.1 Personal identification information (name, job title, email address and/or telephone number/s);

12.2.2.2 Information pertaining to the organizational structure of your company, if applicable.

1.2 The purpose of the processing[6]

The company processes the information referred to above, to:

1.2.1 assist you with a query or request.

6 As defined in section 1 of the POPI Act.

1.2.2 contact you in response to a request for more information on our services.

1.2.3 present to you on a particular service that you have expressed a genuine interest in.

1.2.4 run a proof of concept as a means to demonstrate the effectiveness of our services, where you have requested us to do so.

1.2.5 process the agreement concluded with you and provide you with the services required.

1.2.6 conduct a credit check through an accredited credit bureau, where you intend to conclude a contract with the company.

12.3 A description of the categories of data subjects and of the information or categories of information relating thereto

Categories of Data Subjects	Information Relating Thereto
Employees	Please refer to para 7.1, 7.3.1, 7.6.3 ,7.6.4, 7.8.1 & 7.8.3 above
Suppliers	Please refer to para 7.3.3, 7.4, 7.6.2, 7.6.4, 7.7.2, 7.7.3 & 7.8 above
Customers	Please refer to para 7.6.2, 7.8.1 & 7.8.3 above
Potential Job Candidates	Please refer to para 7.1.1 & 7.8.3 above
Consultants	Please refer to para 7.2, 7.3, 7.4, 7.6.2, 7.6.4, 7.8.1, 7.8.2 & 7.8.3 above
Visitors	Please refer to para 7.8.3 above
Prospective Customers	Please refer to para 7.8.1 & 7.8.3 above
Contractors	Please refer to para 7.2, 7.3, 7.4, 7.6.2, 7.6.4, 7.8.1, 7.8.2 & 7.8.3 above

12.4 The recipients or categories of recipients to whom the personal information may be supplied

Categories of Recipients	Information Supplied to Recipients
Human Resources	Please refer to para 7.1 above
Project Management	Please refer to para 7.2 above
Information Technology	Please refer to para 7.3 above
Catering Department	Please refer to para 7.4 above
Companies Department	Please refer to para 7.5 above
Finance/Accounts Department	Please refer to para 7.6 above
Marketing Department	Please refer to para 7.7 above
Support Services	Please refer to para 7.8 above

12.5 Planned transborder flows of personal information

12.5.1 As a rule, information pertaining to a data subject will not be transferred out of South Africa.

12.5.2 However, where the company services a customer residing in another country, data may be transferred between that country and South Africa. The company will before it transfers information across the South African borders, ensure that the recipient thereof agrees to be bound by the POPI Act under and in terms of binding agreements that provide an adequate level of protection and uphold the principles

for the reasonable and lawful processing of such personal information.

12.6 **A general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the responsible party to ensure that confidentiality, integrity, and availability of the information which is to be processed.**

12.6.1 The company has implemented far-reaching security measures with the assistance of Iris AI (Pty) Ltd. These include, but are not limited to:

12.6.1.1 Physical Security

12.6.1.2 Server security

12.6.1.3 Restrictions on Access

12.6.1.4 Security by design

12.6.1.5 Security objectives established

12.6.1.6 Guidelines published on how to achieve these objectives

12.6.1.7 Adoption of an overall security management strategy

12.6.1.8 Policies on key security mechanisms implemented in both everyday work and serve security.

12.6.2 The totality of the company's security measures is set out in the *Security of Iris AI Services* document, a copy of which is available on the company website www.activetrack.co.za.

13. UPDATING OF MANUAL

The company may update this manual every six months or at such intervals as may be necessary.

Any revision will be published on the company's website. Accordingly, you are advised to visit and re-read this manual on a regular basis.

Active Track (Pty) Ltd
Privacy Policy

Pursuant to the Protection of Personal Information Act, 4 of 2013

Active Track (Pty) Ltd ("Active Track", "we", "us" or "our" as the context may require) is a provider of guard monitoring devices and related security products. Active Track cares about how your personal information is used and is committed to respecting your privacy and helping protect your information.

This Privacy Policy will explain how Active Track uses personal data from you when you use any of our electronic platforms and facilities, including our website, social media, telephone, and/or email ("Active Track's Electronic Facilities") or our services, what information we collect about you, and the corresponding rights and obligations arising in connection therewith.

It is important to note that this Privacy Policy has been drafted in compliance with the Protection of Personal Information Act, 4 of 2013 ("the POPI Act").

PLEASE READ THIS DOCUMENT BEFORE YOU MAKE USE OF ACTIVE TRACK'S ELECTRONIC FACILITIES OR SERVICES OR PROVIDE US WITH ANY PERSONAL INFORMATION. BY PROVIDING ACTIVE TRACK WITH YOUR PERSONAL INFORMATION, YOU AGREE THAT YOU HAVE READ AND UNDERSTOOD THIS PRIVACY POLICY, AND CONSENT TO ACTIVE TRACK PROCESSING YOUR PERSONAL INFORMATION, WHICH WE UNDERTAKE TO PROCESS STRICLTY IN ACCORDANCE WITH THE TERMS OF THIS PRIVACY POLICY.

What data do we collect?

Active Track collects the following data:

- Personal identification information (name, email address, physical address and/or telephone number/s).
- The products and/or services in respect of which you have indicated an interest.

How do we collect your data?

You directly provide Active Track with most of the data we collect. We collect data and process data when you:

- Complete the Contact form on our website, found at www.activetrack.co.za.
- Submit a query or request via Active Track's Electronic Facilities.
- Rent a product from, or subscribe to a service with, us.
- Enter into an agreement with us.
- Voluntarily complete a customer survey or provide feedback on any of our message boards or via email.
- Use or view our website via your browser's cookies.
- Request us to contact you regarding your interest in our products and/or services, via a third party.

How will we use your data?

Active Track collects your data so that it can *inter alia:*

- Assist you with your query or request.
- Contact you in response to your request or query.
- Process any order/s placed with us.
- Arrange delivery of products ordered.
- Process any return of products.
- Improve the quality of our services.
- Recover unpaid sums and/or any other amount due to us.
- Proceed with debt collection.
- Identify other products and/or services which may be of interest to you and informing you of such.
- Consider and/or process applications for re-seller or agency opportunities.

When Active Track processes any applications for re-seller or agency opportunities, it reserves the right to send your data to credit bureaux for purposes of assessing your credit risk. Active Track may base decisions on information obtained from credit bureaux.

In order to correctly handle any query or request, and to perform the abovementioned functions, Active Track may from time to time share your data with its staff, which will only be done on a need-to-know basis; and with its operators including service providers and agents who perform services on behalf of Active Track which will similarly be done on a need-to-know basis, and in terms of an agreement.

Conditions for Lawful Processing

In terms of section 5 of the POPI Act, a data subject has the right to have his, her or its personal information processed in accordance with the conditions for lawful processing. Active Track would like to assure you of its commitment to processing personal information lawfully, and particularly in accordance with the POPI Act. To this end, we wish to make sure that you are aware of the conditions for lawful processing,[1] and have summarised them[2] here:

- **Accountability** – Active Track must ensure that the conditions set out below, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing of personal information and during the processing itself.

- **Processing Limitation** - Personal information must be processed lawfully, and in a reasonable manner that does not infringe on your privacy as data subject. Personal information may only be processed if, given the purpose for which it is processed, is adequate, relevant and not excessive. Furthermore, personal information may only be processed if the data subject consents to the processing; processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party; processing complies with an obligation imposed by law on Active Track; processing protects a legitimate interest of yours; processing is necessary for the proper performance of a public law duty by a public body; or processing is necessary for pursuing the legitimate interests

1 Clause 4 of the POPI Act.

2 While the conditions for lawful processing are all addressed in this document, our summary is intended for informative purposes only. It must not be construed as legal advice or a comprehensive analysis and must not be relied on as such. Where it comes to enforcing your rights, or drafting your own Privacy Policy, independent legal advice by a POPI Act expert is strongly advised.

of Active Track or of a third party to whom the information is supplied.[3] The personal information must be collected directly from you, subject to certain exceptions.[4]

- **Purpose Specification** – personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of Active Track. The records of personal information must not be retained any longer than is necessary for achieving the purposes for which the information was collected or subsequently processed.[5]

- **Further Processing Limitation** – further processing of personal information must be compatible with the purpose for which it was collected.

- **Information Quality** – Active Track must take reasonable steps to ensure that the personal information is complete, accurate, not misleading, and updated.

- **Openness** – Active Track must maintain documentation of all processing operations under its responsibility. In this regard, please refer to the *Manual* available on our website www.activetrack.co.za.

- **Security Safeguards** – Active Track must secure the integrity and confidentiality of personal information in our possession by taking reasonable measures to prevent loss of, damage to or unauthorised destruction of personal information, and unlawful access to or processing of personal information. To this end, please refer to the *Security Measures* document on our website www.activetrack.co.za.

- **Data Subject Participation** – You have the right to request Active Track to confirm whether or not it holds personal information about you and request the record or description of personal information held by Active Track. You may request that we correct or delete inaccurate, excessive, misleading or unlawfully obtained information about you.

How do we store your data?

Active Track securely stores your data with the assistance of its operator Iris AI (Pty) Ltd located at 7 Drome Road, Formain, Johannesburg, Gauteng, South Africa, 2090.

The security measures that have been implemented by Iris AI (Pty) Ltd are far-reaching, and include (but are not limited to):

- Physical Security
- Server security
- Restrictions on Access
- Security by design
- Security objectives established
- Guidelines published on how to achieve these objectives
- Adoption of an overall security management strategy
- Policies on key security mechanisms implemented in both everyday work and server security.

The totality of Iris AI's security measures is demonstrated in the *Security of Iris AI Services* document available on its website www.irisai.co.za. Alternatively, you may request a copy from our Information Officer.

3 For further information, refer to section 11 of the POPI Act.
4 For exceptions, refer to section 12(2) of the POPI Act.
5 For more information, refer to section 14 of the POPI Act.

Active Track will keep your personal identification information, and product preferences until our services and/or communication is no longer required. The default position is to delete your personal data 180 days after either the expiry of your contract with Active Track or your latest interaction with us via Active Track's Electronic Facilities. Once this time period has expired, we will delete your data by shredding and dumping any hard copies of data and destroying the applicable hard drives.

Otherwise, where you have provided data in any of the other circumstances listed under the abovementioned paragraph headed *How will we use your data?,* it will be deleted once our services and/or communication are no longer required. The data will be deleted in the same way as described above.

Marketing

- Active Track would like to send you information about services of ours that we think you may be interested in.
- If you have agreed to receive marketing, you can always opt out at a later date.
- You have the right at any time to stop Active Track from contacting you for marketing purposes.
- If you no longer wish to be contacted for marketing purposes, let us know via the opt-out feature found in the marketing communication, or via email.

What are cookies?

Cookies are text files placed on your computer to collect standard internet log information and visitor behaviour information. When you visit our website, we will collect information from you automatically through cookies or similar technology.

For further information, visit https://www.allaboutcookies.org/.

How do we use cookies?

Active Track uses cookies in a range of ways to improve your experience on our website, including:

- Keeping you signed in on the relevant portal, service, or programme.
- Understanding how you use our website.

What types of cookies do we use?

There are a number of different types of cookies, however, our website uses:

- Functionality – Active Track uses these cookies so that we recognize you on our website and remember your previously selected preferences. These could include what language you prefer and location you are in. A mix of first-party and third-party cookies are used.
- Advertising – Active Track uses these cookies to collect information about your visit to our website, the content you viewed, the links you followed and information about your browser, devices, and your IP address. Active Track reserves the right to share limited aspects of this data with third parties for advertising purposes. We reserve the right to share online data collected through cookies with our advertising partners. This means that when you visit another website, you could be shown advertising based on your browsing patterns on our website.

How to manage cookies

You can set your browser not to accept cookies, and the above website tells you how to remove cookies from your browser. However, in a few cases, some of our website features may not function as a result.

Privacy policies of other websites

Our website may contain links to other websites. Our Privacy Policy applies only to our website, so if you click on a link to another website, you should read their privacy policy.

How to contact us

If you have any questions about Active Track's privacy policy, the data we hold on you, or you would like to exercise one of your rights as a data subject, please do not hesitate to contact our information officer, Stephen Boulton, via one of the following channels:

Email: stephen@activetrack.co.za

Telephone: +27 11 551 1687

Registered Post: 7 Drome Road, Formain, Lyndhurst, Gauteng, South Africa, 2090

Marked for the attention of Information Officer, Stephen Boulton.

Information Regulator

To lodge a complaint pertaining to alleged violations of protection of personal information, you are free to contact the Information Regulator:

Address:	33 Hoofd Street
	Forum III, 3rd Floor Braampark
	Braamfontein, Johannesburg
	2017
Post:	P.O. Box 31533
	Braamfontein, Johannesburg
	2017
Email:	inforeg@justice.gov.za

Changes to our privacy policy

Active Track reserves the right to and may from time to time update this Privacy Policy. Any revision will be published on Active Track's website www.activetrack.co.za.

Accordingly, you are advised to visit and re-read this Privacy Policy on a regular basis.

This Privacy Policy was last updated in February 2021.