

FaceCamAlert (Pty) Ltd



FACECAMLERT

stop crime before it happens

MANUAL PREPARED IN ACCORDANCE WITH SECTION 51 OF THE
PROMOTION OF ACCESS TO INFORMATION ACT 2 OF 2000, AS AMENDED
AND THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

for

FACECAMLERT (PTY) LTD

FaceCamAlert (Pty) Ltd Reg No: 2023/678327/07 VAT No: 4140314537

info@myincidentdesk.com

Information Regulator Registration Number: 0002498/2024-2025-IRRT/PR

Directors: C.J. Janse van Rensburg R Krüger

1 INTRODUCTION

- 1.1 This manual is published pursuant to section 51 of the Promotion of Access to Information Act 2 of 2000 ("**PAIA**") which was promulgated in order to nurture an ethos which promotes transparency, accountability and effective governance of all private and public bodies. PAIA gives effect to section 32 of the Constitution of the Republic of South Africa, 1996, which provides for the right of access to information in a manner that affords persons a means to obtain the records of private and public bodies as promptly and as efficiently as reasonably possible to endorse, including but not limited to, mechanisms and procedures that empower and educate all persons.
- 1.2 PAIA requires organisations to compile a manual as a guide to requesters of information. The manual also serves to indicate the types of records held by FaceCamAlert (Pty) Ltd ("**FaceCamAlert**"/"we"/"us"/"our") and the availability of such records from FaceCamAlert.
- 1.3 In addition, the manual explains how to access, object to, request correction or deletion of, personal information held by FaceCamAlert, in terms of sections 23, 24 and 25 of the Protection of Personal Information Act 4 of 2013 ("**POPIA**"), and the Regulations Relating to the Protection of Personal Information, 2017 ("**POPIA Regulations**").
- 1.4 This manual is not exhaustive of, nor does it comprehensively deal with, every procedure provided for in PAIA. Requestors are advised to familiarise themselves with the provisions of PAIA and POPIA before making any requests to FaceCamAlert in terms of these Acts. However, in terms of section 19 of PAIA, and Regulations 2 and 3 of the POPIA Regulations, FaceCamAlert will provide such assistance as is required in completing the necessary forms, by parties applying for access to information or personal information.

1.5 FaceCamAlert makes no representation and gives no undertaking or warranty that the information in this manual or any information provided by it to a requestor is complete or accurate, or that such information is fit for any purpose. All users of any such information use such information entirely at their own risk, and FaceCamAlert will not be liable for any loss, expense, liability or claims, howsoever arising, resulting from the use of this manual or of any information provided by FaceCamAlert or from any error therein.

2 OVERVIEW OF FACECAMALERT

2.1 FaceCamAlert is a national, centralised facial recognition subscription service providing facial recognition matching and alert services for private properties and businesses. FaceCamAlert achieves this by using the infrastructure such as CCTV cameras, access control and reception management devices of its subscribers to receive images and match it against watchlists of banned individuals or individuals on the SAPS wanted list.

3 INFORMATION OFFICER AND CONTACT DETAILS OF FACECAMALERT

3.1 The Information Officer of FaceCamAlert is Tiaan Janse van Rensburg whose contact details are as follows –

Name	Contact details
Tiaan Janse van Rensburg	Email: info@myincidentdesk.com

4 GUIDE ON HOW TO USE PAIA AND POPIA

4.1 As of 1 July 2021, the Information Regulator has assumed the functions of the South African Human Rights Commission (“**SAHRC**”) and is responsible for PAIA and POPIA queries.

4.2 As part of its functions, the Information Regulator has published a guide on how to use PAIA and POPIA in the new dispensation.

4.3 The Regulator has, in terms of section 10(1) of PAIA, as amended, updated and made available the revised Guide on how to use PAIA (“**Guide**”), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.

4.4 The Guide contains a description of the following:

4.4.1 the objects of PAIA and POPIA;

- 4.4.2 the postal and street address, phone and fax number and, if available, electronic mail address of –
 - 4.4.2.1 the Information Officer of every public body; and
 - 4.4.2.2 every Deputy Information Officer of every public and private body designated in terms of section 17(1) of PAIA and section 56 of POPIA;
 - 4.4.3 the manner and form of a request for –
 - 4.4.3.1 access to a record of a public body contemplated in section 11 of PAIA; and
 - 4.4.3.2 access to a record of a private body contemplated in section 50 of PAIA;
 - 4.4.4 the assistance available from the Information Officer of a public body in terms of PAIA and POPIA;
 - 4.4.5 the assistance available from the Regulator in terms of PAIA and POPIA;
 - 4.4.6 all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging –
 - 4.4.6.1 an internal appeal;
 - 4.4.6.2 a complaint to the Regulator; and
 - 4.4.6.3 an application with a court against a decision by the information officer of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body;
 - 4.4.7 the provisions of sections 14 and 51 of PAIA requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;
 - 4.4.8 the provisions of sections 15 and 52 of PAIA providing for the voluntary disclosure of categories of records by a public body and private body, respectively;
 - 4.4.9 the notices issued in terms of sections 22 and 54 of PAIA regarding fees to be paid in relation to requests for access; and
 - 4.4.10 the regulations made in terms of section 92 of PAIA.
- 4.5 Members of the public can inspect or make copies of the Guide from the offices of the public and private bodies, including the office of the Regulator, during normal working hours.

4.6 Any information or queries related to the guide, or to PAIA or POPIA should be directed to –

Information Regulator

JD House
27 Stiemens Street
Braamfontein
Johannesburg 2001

Website: <https://infoeregulator.org.za/training/wp/enquiries@infoeregulator.org.za>
E-mail: enquiries@infoeregulator.org.za

5 DISCLOSURE IN TERMS OF SECTION 52(1)(a) OF PAIA

The records that are located on the FaceCamAlert website are automatically available to any person requesting this information and it is therefore not necessary to apply for access thereto in terms of PAIA. Our website address where said information or records can be obtained is <https://www.myincidentdesk.com/facecamalert>.

6 RECORDS AVAILABLE IN ACCORDANCE WITH LEGISLATION

Records are kept in accordance with legislation as is applicable to FaceCamAlert, which include (but may not be limited to) the following legislation –

- 6.1 *Basic Conditions of Employment Act 75 of 1997;*
- 6.2 *Broad-Based Black Economic Empowerment Act 53 of 2003;*
- 6.3 *Companies Act 71 of 2008;*
- 6.4 *Compensation for Occupational Injuries and Diseases Act 130 of 1993;*
- 6.5 *Employment Equity Act 55 of 1998;*
- 6.6 *Income Tax Act 58 of 1962;*
- 6.7 *Labour Relations Act 66 of 1995;*
- 6.8 *Occupational Health and Safety Act 85 of 1993;*
- 6.9 *Skills Development Act 9 of 1999;*
- 6.10 *Unemployment Insurance Act 63 of 2001; and*
- 6.11 *Value Added Tax Act 89 of 1991.*

7 DESCRIPTION OF THE SUBJECTS ON WHICH FACECAMLERT HOLDS RECORDS AND CATEGORIES OF RECORDS HELD ON EACH SUBJECT

The following table contains a description of the types of records which FaceCamAlert holds and the categories of records held on each subject –

Subject	Description of record
Statutory records	<ul style="list-style-type: none"> • Company incorporation documents • Share register • Memorandum of Incorporation • Minutes of meetings of the board of directors • Records relating to the appointment of directors, auditors, and other officers
Income tax	<ul style="list-style-type: none"> • Pay-as-you-earn (PAYE) records • Documents issued to employees for income tax purposes • Records of payments made to the South African Revenue Service on behalf of employees • All or any statutory compliance • Value Added Tax • Skills development levies • Unemployment Insurance Fund
Labour relations records	<ul style="list-style-type: none"> • Personnel documents and records • Employment contracts • Medical aid records • Pension Fund records • Disciplinary records

Subject	Description of record
	<ul style="list-style-type: none"> • Salary records • Disciplinary code and / or procedures • Leave records • Training records • Training manuals • Address lists • Internal telephone lists
Finance	<ul style="list-style-type: none"> • Receipts and payments • Bank statements • Budgets • Management accounts • Asset registers • Orders, quotes and invoices • Minutes of meetings • Correspondence
Risk and compliance	<ul style="list-style-type: none"> • Contracts • Testing certificates • Policies and procedures • Risk assessment • Compliance records

8 PROCESSING OF PERSONAL INFORMATION

8.1 POPIA

8.1.1 Chapter 3 of POPIA provides for the minimum conditions for lawful processing of personal information. These conditions may not be derogated from unless specific exclusions apply as outlined in POPIA.

8.1.2 FaceCamAlert processes personal information in accordance with POPIA. In terms of our Internal Privacy Policy and External Privacy Notice, FaceCamAlert will ensure that all processing conditions of POPIA are complied with at the time of processing of personal information. FaceCamAlert processes personal information of both natural and juristic persons.

8.2 Purpose of processing personal information by FaceCamAlert

As stated in our Privacy Notice, FaceCamAlert processes personal information for a number of reasons including –

IN RESPECT OF EMPLOYEES	IN RESPECT OF CUSTOMERS/PARTNERS, THE GENERAL PUBLIC AND SERVICE PROVIDERS
Concluding employment contracts	Concluding contracts
Human Resource and Finance functions e.g. recruitment, payroll, audit functions, etc.	Conducting due diligence checks
Disciplinary/Grievance processes	Onboarding
Training and development	Payment of invoices
Regulatory compliance	Communication
Record keeping	Providing CCTV surveillance services

8.3 Categories of data subjects and their personal information

Internal personal information (employees)	
Full name and surname	Physical address
Identity/passport copy	Cell phone number
Email address	Tax details
Banking details	Marital status

Gender	Payroll information
Nationality	Education and employment history
Age	Next of kin/emergency contact details
Income tax information/IRP5 forms	CCTV footage
Disciplinary records (e.g. warnings, suspensions, etc.)	Curriculum Vitae (CV)
References	Employment performance details (e.g. management reviews)
Pension fund details	IP address, usernames, passwords, device and internet usage details
Employment agreements	Confidentiality agreements
Passwords and computer usage data	Active Directory Logins
PSIRA certification	Polygraph test results
Internal special personal information (employees)	
Race (for B-BBEE purposes)	Health status and records (e.g. medical aid membership information, chronic conditions, allergies, disability, etc.) for emergency and employment equity Purposes
Criminal history (background checks)	Biometric data (e.g. fingerprints used to enter FaceCamAlert offices) – these are removed from the system as soon as an employee is no longer under the employ of FaceCamAlert
External personal information (Customers/Partners and Service Providers)	
Full name and surname	ID/Passport number or company registration number
Tax certificate and B-BBEE status/certificate	CIPC certificates
Nationality	Contact information (cell/telephone number, email address)
Physical address	Confidentiality agreements
Banking details	Contracts
PSIRA documentation and ID numbers (to set-up the clients and give access to its internal systems)	Customer agreements and independent contractor agreements

External personal information (General Public including visitors to FaceCamAlert's premises)	
CCTV Footage	Vehicle registration plates
Images of vehicles linked to relevant number plate (no details of the owners linked to the number plates are processed)	Access to all camera feeds and databases by support for monitoring watchlist matches
Images of face of people entering the premises for matching against watchlists. If no match is found the details and image of the person's face is immediately deleted.	

External personal information (Data subjects included on watchlists)	
CCTV Footage	Image of possible facial recognition matches.
Name and surname of data subject.	List of crime(s) or transgression(s) of which the data subject has been found guilty, has admitted guilt to, or is a suspect of.
Images of face of data subject. If no match is found the details and image of the person's face is immediately deleted.	Case numbers and warrant of arrest number.

8.4 Disclosure of your personal information

We may share information about you with –

- 8.4.1 companies which are affiliated with FaceCamAlert;
- 8.4.2 partners, agents or suppliers involved in delivering the services you have requested from us;
- 8.4.3 partners or agents that conduct customer satisfaction surveys and any other surveys related to the products or services provided to you;
- 8.4.4 companies who are engaged to perform services for or on behalf of FaceCamAlert;
- 8.4.5 debt collection agencies or other debt recovery organisations;

- 8.4.6 law enforcement agencies, regulatory organisations, courts or other public entities if we are required by law to do so;
- 8.4.7 emergency services;
- 8.4.8 with any entity or forum wherein we may protect ourselves against fraud or exercise our rights; and
- 8.4.9 if we are reorganised or sold to another organisation, we may transfer any personal information we hold about you to that organisation.

8.5 Transborder/Cross-border flows of personal information

Section 72 of POPIA provides that personal information may only be transferred out of the Republic of South Africa if certain conditions are satisfied. FaceCamAlert currently has no planned transborder flows of personal information. Insofar as the transborder flow of personal information may become applicable in future, FaceCamAlert will comply with the conditions set out in section 72 of POPIA.

8.6 General description of information security measures

- 8.6.1 FaceCamAlert takes reasonable and appropriate technical and organisational measures to ensure that personal information is kept secure and is protected against unauthorised or unlawful processing, accidental loss, destruction or damage, alteration disclosure or access. We contractually require that service providers who handle your personal information for us do the same.
- 8.6.2 FaceCamAlert, on a regular basis, reviews the security controls and related to processes to ensure that personal information is secure.
- 8.6.3 Some of the controls we have in place are that we use digital environments to host the communications infrastructure that makes up the watchlist network and matching platform–
- 8.6.4 FaceCamAlert uses protected data storage system and its firewalls are regularly updated;
- 8.6.5 FaceCamAlert's tech firmware and software is updated regularly and patched up;
- 8.6.6 FaceCamAlert's networks are private and can be accessed over a private VPN service that encrypts all traffic in terms of industry best practices;
- 8.6.7 legal documents are stored on a cloud-based server with access granted only to certain individuals;

- 8.6.8 FaceCamAlert uses various software programs in respect of its facial recognition match processing and storage facilities;
- 8.6.9 the facial recognition matches are located on FaceCamAlert's systems in accordance with FaceCamAlert's footage request process which, if requested for use as evidence in a case, must be accompanied by a case number;
- 8.6.10 servers are monitored in real time to limit the risk on infrastructure systems;
- 8.6.11 patch maintenance is carried out regularly;
- 8.6.12 firewall systems are in place;
- 8.6.13 audits are regularly conducted to ensure that there has been no leakage of information or hacking;
- 8.6.14 FaceCamAlert audits its clients' access to its systems and further requests updated lists of operators from clients to update said access;
- 8.6.15 FaceCamAlert has further identified some foreseeable internal and/or external risks such as
 - 8.6.15.1 the risk of being hacked; and

9 HOW TO REQUEST ACCESS TO A RECORD

- 9.1 To request a record in terms of PAIA, the requestor must complete the prescribed form attached to this manual as **Annexure A**. This request must be sent to the Information Officer at the addresses provided at paragraph 3.1.
- 9.2 For POPIA-related requests to object to the processing of personal information, correct or delete personal information, the request must be made in writing on the applicable prescribed **Form 1** (objection) or **Form 2** (correction or deletion), which are attached to this Manual as **Annexure B**.
- 9.3 The requestor must provide sufficient detail to enable the Information Officer to identify the record(s) requested and the requestor. The requestor must indicate which form of access is required, identify the right that he/she is seeking to exercise or protect and provide an explanation of why the requested record is required for the exercise or protection of that right.
- 9.4 If the request is made on behalf of another person, the requestor must submit proof of the capacity in which the requestor is making the request, to the reasonable satisfaction of the Information Officer.

9.5 PAIA makes provision for certain grounds upon which a request for access to information must be refused. On this basis, the Information Officer will decide whether or not to grant a request for access to information.

10 PAYMENT OF FEES

10.1 PAIA provides for two types of fees, namely –

10.1.1 a request fee, which will be a standard non-refundable administration fee, payable prior to the request being considered; and

10.1.2 an access fee, payable when access is granted which must be calculated by considering reproduction costs, search and preparation time and cost, as well as postal costs.

10.2 Subsequent to a request being made, the Information Officer, shall by notice require the requester, excluding personal requester, to pay the prescribed request fee (if any) before further processing of the request.

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

10.4 FaceCamAlert may withhold a record until the requester has paid the fees as indicated.

10.5 **Annexure C.**

10.6 A requester whose request has been granted must pay the applicable access fee for reproduction, search, preparation and for any time reasonably required in excess of the prescribed hours to search for and prepare the record for disclosure including making arrangements to make it available in the request form.

10.7 In terms of POPIA, a data subject has the right to request FaceCamAlert to confirm, free of charge, whether or not it holds personal information about the data subject and request from FaceCamAlert the record or a description of the personal information held, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information.

10.8 POPIA further provides that where the data subject is required to pay a fee for services provided to them, FaceCamAlert must provide the data subject with a written estimate of the payable amount before providing the service and may require that the requestor pay a deposit for all or part of the fee.

11 **APPLICABLE TIME-PERIODS**

11.1 FaceCamAlert will inform the requester within 30 days after receipt of the request of its decision whether or not to grant the request.

11.2 The 30-day period may be extended by a further period of not more than 30 days if the request is for a large number of records or requires a search through a large number of records and compliance with the original period would unreasonably interfere with the activities of FaceCamAlert or the records are not located at FaceCamAlert.

12 **OUTCOME OF THE REQUEST (GRANTING OR REFUSING)**

Should the request be refused, the notice will state adequate reasons for the refusal, including the provisions of the PAIA relied upon; and that the requester may lodge an application with a court against the refusal of the request.

13 **GROUND FOR REFUSAL OF ACCESS TO RECORDS**

13.1 In terms of sections 62 to 69 of PAIA access granted to a record may be refused on one or more of the following grounds –

13.1.1 protection of privacy to a third party who is a natural person;

13.1.2 protection of the commercial information of a third-party;

- 13.1.3 protection of certain confidential information of a third-party;
 - 13.1.4 protection of the safety of individuals and the protection of property;
 - 13.1.5 protection of records privileged from production and legal proceedings;
 - 13.1.6 the commercial information of FaceCamAlert;
 - 13.1.7 the protection of research information of a third-party, and protection of research information of a FaceCamAlert.
- 13.2 Despite any provisions of PAIA, a request must be granted if the disclosure of the record would reveal evidence of substantial contravention of, or failure to comply with, the law or imminent and serious public safety or environment risk, and the public interest in the disclosure of the record clearly outweighs the harm contemplated (section 70 of PAIA).

14 **REMEDIES FOR REFUSAL**

Should the requester be dissatisfied with the Information Officer's decision to refuse access, that person may within 30 days after notification of the refusal apply to a court for the appropriate relief.

15 **AVAILABILITY OF THE MANUAL**

This manual is available in electronic format in English. The electronic version of this manual is available on the website of FaceCamAlert accessible at <https://www.myincidentdesk.com/facecamalert>.

16 **UPDATING OF THIS MANUAL**

This manual will be reviewed and updated, if necessary, on a periodic basis.

ANNEXURE A
FORM C
REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY
(Section 53(1) of the Act) [Regulation
10]

A. Particulars of private body

The Head: _____

Company Name: _____

Company Registration Number: _____

B. Particulars of person requesting access to the record

- (a) The particulars of the person who requests access to the record must be given below.*
- (b) The address and/or fax number in the Republic to which the information is to be sent must be given.*
- (c) Proof of the capacity in which the request is made, if applicable, must be attached.*

Full names and surname: _____

Identity number: _____

Postal address: _____

Fax number: _____

Telephone number: _____

E-mail address: _____

Capacity in which request is made,

when made on behalf of another person: _____

C. Particulars of person on whose behalf request is made

This section must be completed ONLY if a request for information is made on behalf of another person.

Full names and surname: _____

Identity number: _____

Postal address: _____

Fax number: _____

Telephone number: _____

E-mail address: _____

D. Particulars of record

- (a) *Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located.*
- (b) *If the provided space is inadequate, please continue on a separate folio and attach it to this form. **The requester must sign all the additional folios.***

1. Description of record or relevant part of the record:

2. Reference number, if available:

3. Any further particulars of record:

E. Fees

- (a) *A request for access to a record, other than a record containing personal information about yourself, will be processed only after a **request fee** has been paid.*
- (b) *You will be notified of the amount required to be paid as the request fee.*
- (c) *The **fee payable for access** to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.*
- (d) *If you qualify for exemption of the payment of any fee, please state the reason for exemption.*

Reason for exemption from payment of fees:

F. Form of access to record

Not available.

G. Particulars of right to be exercised or protected

*If the provided space is inadequate, please continue on a separate folio and attach it to this form. **The requester must sign all the additional folios.***

1. Indicate which right is to be exercised or protected:

2. Explain why the record requested is required for the exercise or protection of the aforementioned right:

H. Notice of decision regarding request for access

You will be notified in writing whether your request has been approved/denied. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decision regarding your request for access to the record?

Signed at _____ this _____ day of _____ 20 _____

Signature of requestor /
person on whose behalf request is made

Name of requestor /
person on whose behalf request is made

ANNEXURE B

FORM 1

**OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF
SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013
(ACT NO. 4 OF 2013)**

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017
[Regulation 2(1)]

Note:

- 1. Affidavits or other documentary evidence in support of the objection must be attached.*
- 2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*

Reference Number.....

A	DETAILS OF DATA SUBJECT
Name and surname of data subject:	
Residential, postal or business address:	
Contact number(s):	
FAX number:	
E-mail address:	
B	DETAILS OF RESPONSIBLE PARTY
Name and surname of responsible party <i>(if the responsible party is a natural person):</i>	

Signed at this day of 20.....

Signature of Data subject (applicant)

FORM 2

**REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR
DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF
SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013
(ACT NO. 4 OF 2013)**

**REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017
[Regulation 3(2)]**

Note:

*Affidavits or other documentary evidence in support of the request must be attached.
If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and
sign each page.*

Reference Number.....

Mark the appropriate box with an "x".

Request for:

Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	DETAILS OF DATA SUBJECT
Surname:	
Full names:	
Identity number:	
Residential, postal or business address:	

Contact number(s):	
FAX number:	
E-mail address:	
B	DETAILS OF RESPONSIBLE PARTY
Name and surname of responsible party <i>(if the responsible party is a natural person):</i>	
Residential, postal or business address:	
Contact number(s):	
FAX number:	
E-mail address:	
Name of public or private body <i>(if the responsible party is not a natural person):</i>	
Business address:	
Contact number(s):	
FAX number:	
E-mail address:	

FEES PAYABLE IN RESPECT OF RECORDS REQUESTED FROM FACECAMALERT

ANNEXURE C

	DETAILS OF REQUEST	COST
1	Standard fee for any request to be processed regardless of success of request.	R200
2	If successful the following amount is payable for the provision of feedback, footage and documentation where applicable.	R400