# FaceCamAlert (Pty) Ltd

FACECAMALERT

stop crime before it happens

## FACIAL RECOGNITION MATCHING POLICY - MARCH 2024

for

## FACECAMALERT (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

## ANNEXURES

### ANNEXURE A – INTERPRETATION

## 1 INTRODUCTION

1.1 FaceCamAlert is a national, centralised facial recognition subscription service providing facial recognition matching and alert services for private properties and businesses for security and commercial purposes. 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.

1.2 The facial recognition matching services are provided to pre-vetted and approved companies which provide security services usually on behalf of residents' associations, property owners and managers, and companies in the insurance and financial services industries to counteract fraud and enforce other rights afforded to them under statute and contract.

1.3 The facial recognition devices are positioned so that they record private property. Footage of these areas is not recorded or stored. Information of data subjects who are not on the watch list will not be stored. If a data subject passes a facial recognition camera and no match is found against a watchlist then their data is immediately deleted.

1.4 It is our commitment to our employees, directors, affiliates, partners and/or clients and members of the general public to continually implement practices and procedures that respect and give effect to your right to privacy. Therefore, we have compiled this Facial Recognition Policy ("**FR Policy**") to ensure our commitment to your privacy and compliance with the applicable laws and regulations, in particular the *Protection of Personal Information* Act 4 of 2013 ("**POPIA**").

## 2 PURPOSE

2.1 We recognise that everyone has the right to privacy which includes protection against the unlawful collection, retention, dissemination and use of personal information. Consequently, this FR Policy sets out to –

2.1.1 promote ethical standards including, but not limited to, protecting your personal information, respecting your individual privacy, guarding against security threats and maintaining best practices with regards to CCTV surveillance;

2.1.2 explain how we will collect through the CCTV infrastructure of our subscribers (the responsible party), process and store your personal information in a reasonable manner;

2.1.3 clarify the practices and procedures that will enable us to monitor and audit compliance with this FR Policy;

2.1.4 provide guidelines on processing personal information where doing so would protect the legitimate interests of the responsible party and enhance their safety and that of FaceCamAlert;

2.1.5 advise individuals of their rights and remedies under POPIA; and

2.1.6 minimise the inherent risks of non-compliance with the relevant law and regulations, including but not limited to, privacy infringement, reputational damage and regulatory sanctions.

## 3 APPLICATION OF POLICY

This FR Policy applies to FaceCamAlert and all of our employees, directors, affiliates, partners and/or clients.

## 4 ACCOUNTABILITY

4.1 The authorisation for the collection, location and access to the FR matching records lies with us as permitted by the relevant lawful bases. As such, the personal information may be accessed through our systems and only with our express prior written consent. Moreover, such access will only be granted to pre-vetted, third-party companies such as a security services providers in line with the applicable legislative and regulatory requirements.

4.2 FaceCamAlert shall fully comply with its obligations in terms of POPIA and any company appointed by FaceCamAlert will be required to act within the prescripts of the law.

4.3 FaceCamAlert further commits to process personal information where, given the purpose for which it is processed, such processing is adequate, relevant and not excessive.

4.4 Any unlawful disclosure of personal information, or data breach, will be reported to the Information Regulator, together with all details relating to the breach as required by POPIA.

## 5 SCOPE AND OPERATION OF CCTV SURVEILLANCE NETWORK

5.1 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.

5.2 The FR matching data will only be made available in a manner consistent with the requirements and restrictions imposed by POPIA, whilst always considering each individual's right to privacy.

5.3 All FR matching data shall be reviewed by the operational staff employed by the Responsible Parties/subscribers who will monitor the FR matches for appropriate purposes which may include, but are not limited to –

5.3.1 assisting in the identification and prevention of criminal activity;

5.3.2 upholding and/or enhancing the interests of public safety and security;

5.3.3 assisting in fraud prevention, loss prevention and asset protection; and

5.3.4 assisting various parties, as the case may be, in enforcing their rights under statute or law.

## 6 FACECAMALERT AND YOUR PERSONAL INFORMATION

6.1 We will be primarily responsible for processing your personal information either as a

responsible party or operator. In this regard we undertake to fully comply with the obligations of POPIA, depending on the capacity in which we are acting in any given circumstance.

6.2 We will mainly process your personal information in the following respects –

| Employees/Directors/Affiliates/Partners/Clients/General Public | | |
|---|---|---|
| **What We Process** | **Why We Process** | **Legal Basis** |
| Images of face of people entering the premises. For matching against suspect wanted lists. If no match is found the details and image of the person's face is immediately deleted. | For matching against suspect wanted lists. If no match is found the details and image of the person's face is immediately deleted. | The grounds for processing are that it is the legitimate interest of the customer, i.e. the occupier of the premises to keep the premises secure and to guard against offences and misdemeanours commonplace to such premises. These are usually crime, damage to property and trespassing to name a few. |

6.3 Personal information collected by our FR matching service will not be used for any other purposes other than those listed above or as permitted by law.

## 7 SPECIAL PERSONAL INFORMATION

7.1 We understand that through our FR matching service, we may be able to establish certain facts relating to your race, for example. The information about the race of data subjects is not captured separately on the watchlist or alerts, and can only be deduced from the photographs on the watchlist / alerts. This information is also only used to identify the data subject to make a match between the alert and the person on site, and such identification is integral to the purpose (section 29(a)). Watchlist are also not created and differentiated based on race.

7.2 Processing information about children is generally not permitted. Section 35(1)(b) of POPIA provides that information about children may be processed, amongst others, if it is necessary to exercise a right in law. The customers of FCA have a right to protect their premises against theft, vandalism and robbery, and if children are involved in such crimes, such processing is permissible. If children are regularly involved in such crimes the Responsible party (subscriber) must first obtain authorisation from the Information Regulator in terms of section 35(2) of POPIA.

## 8 SECURITY SAFEGUARDS

8.1 The data is stored on a secure server(s) in a secure hosted data center with all necessary security measures in place.

8.2 Access to the data center and server(s) are secure and managed.

8.3 The data subject personal information is secured against loss and unlawful access.

8.4 We adopt a "need to know" approach to access to our CCTV surveillance footage. Individuals who have such access include, from time to time –

8.4.1 our relevant security personnel/service providers;

8.4.2 our Information Officer;

8.4.3 support staff required to support, service or maintain the surveillance network; and

8.4.4 any other employee or service provider appointed by us who may, from time to time, require access to the system in fulfilment of the purposes of this Policy or any

mandate related to their core functions.

## 9 DATA SUBJECT CONSENT

9.1 The grounds for processing are that it is the legitimate interest of the customer, i.e. the occupier of the premises to keep the premises secure and to guard against offences and misdemeanours commonplace to such premises. These are usually crime, damage to property and trespassing to name a few.

## 10 DATA SUBJECT RECORDS

10.1 A severity level framework is utilised to differentiate between data subjects in different watchlist. SubjectS in different watchlist are treated differently. Records of data subject in different watchlists are retained for a period applicable to that watchlist and range between a period of 3 months to 60 months from the date the last incident has been loaded in respect of the data subject.

10.2 Records of alerts are retained for 30 days.

10.3 No records are retained of persons who are not on the watch list.

## 11 FURTHER PROCESSING

11.1 The information will not be processed for any other purpose than the stated purpose of protecting the premises and preventing crime and illegal activity.

11.2 Each customer/subscriber is a Responsible Party in own right and have their own segregated watchlist.

## 12 WHEN WILL INFORMATION BE FURTHER PROCESSED

12.1 Section 15 of POPIA provides that further processing is permitted when the further processing is compatible with the original purpose and sets out a few criteria to determine compatibility:

12.1.1 The original purpose and the purpose of further processing is exactly the same as each customer maintains a watchlist for crime prevention (section 15(2)(a)).

12.1.2 The potential consequences for subjects of interest are the same when the incident information is shared, in other words the customer will initiate appropriate steps to monitor or escort the subject from the premises or inform law enforcement if necessary (section 15(2)(c)).

12.1.3 The customers do not have contractual relations with one another but their agreements with FCA must include provisions to bind them to a set of rules for uploading information to their watchlists and to regulate their use of information received from other watchlists (section 15(2)(e)).

12.1.4 Information that is derived from a public record is also allowed to be further processed (section 15(3)(b)).

12.1.5 Further processing is allowed if it is necessary to enable a public body to prevent, detect, investigate or prosecute offences (section 15(3)(c)(i)).

12.2 When information from other databases is used for matching or alerts, FCA will evaluate the purpose of that specific database, and if relevant the laws in terms of which that database operates, to make an assessment for each such source database whether further processing is compatible with the original purpose.

12.3 FCA takes the following steps to mitigate the potential privacy risks:

12.3.1 Designated users cannot freely make enquiries against its own watchlists or the watchlists of others. It can only make enquiries if the subject has been detected on site by the cameras;

12.3.2 Queries can only be made within a set time limit after being detected by a camera;

12.3.3 No customer, designated user or FCA employee can follow a subject's movement across different customers premises;

12.3.4 Alerts with the additional information is only available for a limited duration on the system.

## 13 QUALITY OF INFORMATION

13.1 The following processes are in place to ensure the information of data subjects on the watchlist is accurate:

13.1.1 Quality checks are provided by the facial recognition system before uploading an image of a data subject;

13.1.2 Quality checks are provided by the facial recognition system before releasing the alert.

## 14 ACCOUNTABILITY

14.1 The customer is the responsible party in respect of the processing and FCA acts as the operator.

14.2 The customer decides on the purpose for the processing, namely to keep its premises secure and to prevent illegal activity. The customer selects the FCA solution as the means of processing.

14.3 FCA has no relationship with the data subjects, whereas the customer either encounters data subjects on its premises or had prior interaction with the data subjects.

## 15 SHARING OF INFORMATION

We may share or transfer your Personal Information as follows or as otherwise described in this Policy –

15.1 with our customers, affiliates and/or partners who only have access to such information as is necessary to perform their functions or give effect to an agreement to which you are a party or legal obligation and not any other purpose;

15.2 any operators will act on our instructions and be contractually bound to take all reasonable steps to protect your personal information;

15.3 in response to a request for information if we believe disclosure is in accordance with any applicable law, regulation, or legal process, or as otherwise required by any applicable law, rule or regulation; and

15.4 in connection with, or during negotiations of, any merger, sale of our assets, financing, or acquisition of all or a portion of our business to another company (we will request a purchaser to treat our data under the privacy/confidentiality statement in place at the time of its collection).

## 16 CROSS-BORDER INFORMATION TRANSFERS

Where we transfer personal information about you to a company or any other entity outside of South Africa, we will ensure that –

16.1 the company receiving the information is subject to a law, binding corporate rules or a

binding agreement which provides an adequate level of protection of your personal information; and/or

16.2 we obtain your consent if need be; and/or

16.3 there is a contractual necessity/obligation to transfer the personal information.

## 17 YOUR RIGHTS

17.1 You have a number of rights under law which, in certain circumstances, you may exercise in relation to the personal information we process about you. these include –

17.1.1 the right to access a copy of the personal information that we have about you;

17.1.2 the right to correction of inaccurate personal information we hold about you;

17.1.3 the right to restrict our use of your personal information;

17.1.4 the right to request that your personal information be deleted; and

17.1.5 the right to object to our use of your personal information.

17.2 Where we rely on consent as the legal basis on which we process your personal information, you may also withdraw that consent at any time.

## 18 WHO TO CONTACT IN CASE OF CONCERNS

18.1 We have designated an Information Officer who shall be responsible for –

18.1.1 the administration of this Policy and ensuring the lawful processing of personal information by ourselves;

18.1.2 dealing with requests made to us for access to personal information held by us;

18.1.3 conducting annual reviews of our alerting service and usage;

18.1.4 liaising with regulators; and

18.1.5 providing training to our employees.

18.2 should you wish to raise any questions, concerns or reportable conduct, please contact our Information Officer at –

info@FaceCamAlert.co.za

## 19 CONSEQUENCES OF NON-COMPLIANCE

19.1 Any contravention(s) of this Policy may result in disciplinary action being instituted against an employee, which action may include dismissal or termination of employment and any other legal action that may be available to us.

19.2 we also reserve the right to exercise any appropriate form of legal action against any party which may cause us harm and/or damages by way of non-compliance with this CCTV Policy. Parties also risk statutory penalties.

## 20 OPENNESS

20.1 Where this service is deployed FaceCamAlert will take all reasonable steps to ensure that the Responsible party places the necessary signage at the property entrance where the service is being utilized.

20.2 This Policy, along with our Privacy Notice and PAIA will also be made available on our publicly accessible website at https://www.FaceCamAlert.co.za/.

## 21 POLICY REVISION

This Policy is subject to review and amendment without prior notice. However, we undertake to ensure that any amendments hereto are communicated clearly and effectively, for the benefit of the persons who may be affected by this Policy.

## 22 VERSION CONTROL

Last updated **August 2024**.

## ANNEXURE A – INTERPRETATION

### 1 INTERPRETATION

For the purposes of this CCTV Policy, the following definitions apply –

1.1 "**Consent**" means an informed, unconditional, specific and voluntary expression of will in terms of which permission is given for the processing of personal information.

1.2 "**Data Subject**" means the natural or juristic person to whom personal information relates.

1.3 "**Employee**" means any such person as defined in the Labour Relations Act 66 of 1995, under the employ of FaceCamAlert, and any other such person who may conduct work for or on behalf of FaceCamAlert on a once off or ongoing basis, as the case may be.

1.4 "**Information Officer**" means the person/s designated by us to direct compliance with POPIA within our company.

1.5 "**Legal Obligation**" – means we are required by law to process your personal information.

1.6 "**Operator**" means any person who processes personal information for or on behalf of ourselves in terms of a contract or mandate concluded between ourselves and such person.

1.7 "**Process/Processing**" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, and includes the meaning given to it in the POPIA.

1.8 "**Responsible Party**" means any public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.