



- /Administration
- /Human Resources
- /Legal
- /Accounting
- /Finance
- /Marketing
- /Publicity
- /Promotion
- /Research
- /Business
- /Development
- /Engineering
- /Manufacturing
- /Planning



# *Automated Facial Recognition*

## **A guide to ethical and legal use**




# Contents



Why AFR?	3
How is AFR used?	4
How to apply this guidance	6
Assessing the need for AFR	6
Terms, definitions & abbreviations	7
Governance & Compliance	8
Operational Requirement	9
Data privacy	10
Storage & retention	10
Reference database	11
Verification - is it you?	12
Identification - who is it?	13
Useful references	14

*BSIA Artificial Intelligence Series*  
**BSIA Form 347 | Issue 1 | January 2021**

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.



# Why AFR?

Automated Facial Recognition (AFR) is a technology that has been designed to improve the safety and wellbeing of people, as well as providing a tool to assist and speed up operational processes. AFR is one of many data analysis technologies which sit under the overarching umbrella of Artificial Intelligence (AI), a branch of Computer Science.

The ethics of AI and its application need to be regularly reviewed to ensure that it is not allowed to act autonomously without human oversight and it should not be used in any way which causes harm to individuals.

There is no single global ethical framework for the safe use of AI, therefore we refer to the [Organisation for Economic Cooperation and Development \(OECD\)](#) recommendations which identify five complementary [values-based principles](#) for the responsible stewardship of trustworthy AI:

**AI should benefit people and the planet by driving inclusive growth, sustainable development and wellbeing.**

**AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards, e.g. enabling human intervention where necessary to ensure a fair and just society.**

**There should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them.**

**AI systems must function in a robust, secure and safe way throughout their life cycles and potential risks should be continually assessed and managed.**

**Organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles.**

AFR is one of many different types of AI technologies, each of which perform specific tasks for example, detect objects in images, recommend movies, examine research papers, work out trends and forecasts and write prose. The applications for AI span across multiple sectors from healthcare to manufacturing to retail.



## How is AFR used?

AFR is used in different scenarios by a wide range of organisations across multiple sectors. It is capable of finding a face in an image and mapping the features to create a pattern. This pattern can then be matched against other images that are stored within a database to either verify a high level of likeness (e.g. check against a passport photo; controlled environment), or identify as being present in a specific location at a particular time (e.g. a person of interest at a public event - dynamic environment) if their image is held in a general database.

Once the verification or identification process has taken place, the authentication is then confirmed by either the AFR technology or passed

to a human to make the decision (to confirm the recognition and either action or do nothing), which process is dependent on the specific scenario and operational requirements.

Generally, AFR technology confirms authentication where the data has been willingly supplied and is being actioned within a controlled environment. In contrast, a human confirms authentication for mass surveillance where the subject is not necessarily aware of observation or where AFR is deployed within a dynamic environment.\*

*\*see AFR purpose/decision diagram, page 9*

## **IMPORTANT - READ THIS!**

### **ETHICAL CONSIDERATIONS FOR SPECIFIC USE OF AFR**

**AFR should not cause harm to any individual. Harm means a negative impact on privacy, dignity and human rights.**

**When using AFR, the necessary risk assessment and Data Protection Impact Assessment (DPIA) should be undertaken.**

**Relevant training must be given to staff who may need to authenticate an AFR verification.**

**Instances where AFR could have a negative impact on the individual should result in the authentication process being confirmed by a human.**

# AFR SHOULD NOT DISCRIMINATE

The technology within AFR cannot be inherently biased. It is how it is trained and how it is used which determines how accurate it may be in detecting features from the widest demographic in a range of lighting scenarios.

Inaccurate decisions that may be perceived as bias in the AFR system, for example difficulty in recognising faces from a diverse demographic, should be reported to the AFR provider who in turn should take immediate corrective action.

If there is an adverse impact on individuals who are not recognised, an alternative method of authentication should be considered.

Discrimination can be a concern when using AFR systems and for this document it should be advised that the choice of software used to analyse the captured image should be carefully considered. We recommend that internationally respected organisations such as NIST in the USA, who publish the results of their tests online, may be consulted.



## AFR SHOULD BE USED TRANSPARENTLY TO ENABLE THE PERSON TO PROVIDE CONSENT TO THE USE OF THEIR PERSONAL DATA

The AFR training data should be obtained lawfully and within overarching ethical and legal guidelines.

The database of images against which the AFR matches faces must be legally controlled as set out in the **Data Protection Act 2018**, incorporating the **General Data Protection Regulation (GDPR)**. It must be possible for an individual to find out if they are on a watch list through subject access requests or other legal means. It must be clear to the individual that they are giving consent by using an area controlled using AFR.

Images of people are a 'biometric' identifier of a person, and as such are legally referred to as '**Special Category**' data, which invokes additional requirements under the DPA 2018 and GDPR.

The use of AFR should be proportionate to the purpose i.e. the problem being solved. There must be a lawful basis for processing personal data and it should be considered whether the same objective can be achieved by other less intrusive measures.



# How to apply this guidance

This guidance **provides advice and recommendations** on the ethical and legal use of AFR technology for beneficial use in both public and private sector environments to ensure it does not **cause harm or discriminate** against persons.

It takes into account current known legislation, standards and guidance around AI and in particular AFR.

It is intended to be useful to system designers, installers/integrators and end-users.

**This guidance does not cover the technical elements of AFR technology, and these are covered in other published standards.**

## Assessing the need for AFR

There are important early stage decisions which need to be made before the AFR is deployed taking into account the following steps:

Define **why** AFR is needed

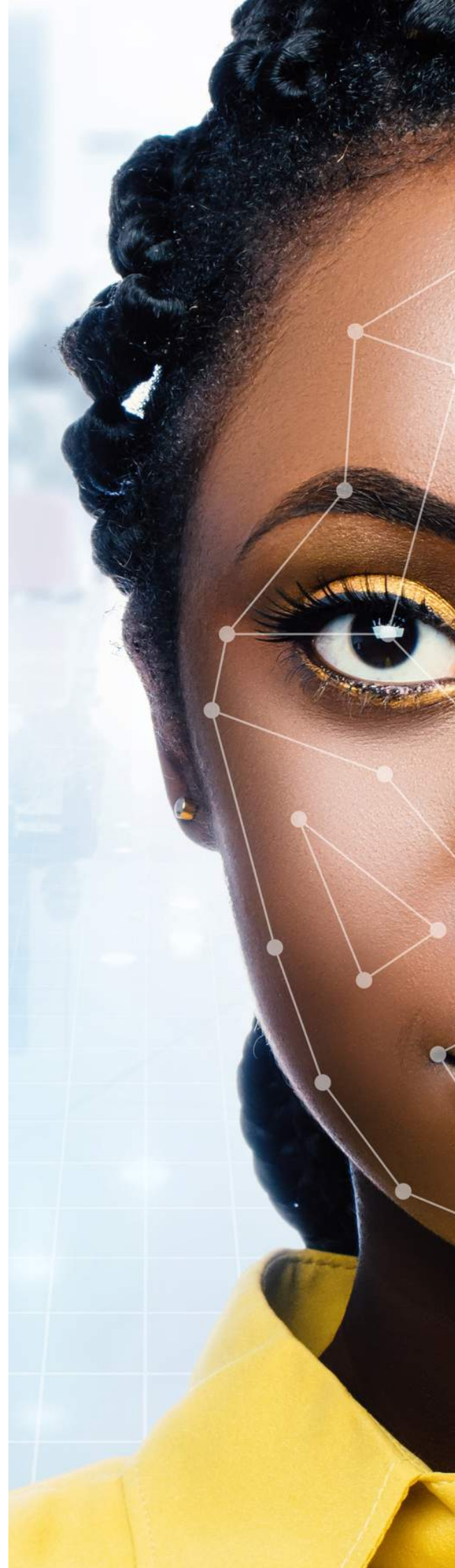
Define **where** AFR will be used

Define the **purpose** of its use

Undertake an **ethical assessment based on OECD** guidelines

Undertake a **DPIA** and ensure ethical and legal compliance and proportionality

If the **location and purpose of the AFR is legal, ethical and proportionate**, you are ready to create an operational requirements specification.



# Terms, definitions & abbreviations

## **Authentication**

The process or action of proving or showing something to be true, genuine, or valid

## **Identification**

The action or process of identifying someone or something

## **Operator**

Individual(s) responsible for the day to day operation of the system

## **Artificial Intelligence (AI)**

The ability for machines to interpret and learn from data to make a prediction without being explicitly programmed to do so.

## **Automated Facial Recognition (AFR)**

A software application that is capable of uniquely identifying or verifying a person by comparing and analysing patterns based on a person's facial contours against a digital image or a video frame from a video source.

## **Data**

Personal information which relates to an identified or identifiable natural person.

## **Training data**

Personal information relating to an identified or identifiable natural person that is stored by the AFR system to assist in its ability to correctly compare and identify the same person.

## **Watchlist\***

A list of individuals, groups, or items that require observation, typically for legal or political reasons

## **Verification**

One to one matching of the image of a face with the identity to verify it is the individual.

## **Abbreviations**

**AFR** Automated Facial Recognition

**AI** Artificial Intelligence

**DPIA** Data Protection Impact Assessment

**GDPR** General Data Protection Regulation

**OECD** Organisation for Economic Cooperation and Development

**VSS** Video Surveillance System

\*The words database and watch-list in the context of this document are interchangeable.

# Governance & compliance

## Accountability

Ensure an individual or group is **nominated and held accountable** for the ethical and legal compliance and operation of the system.

Ensure there is an **ethical and lawful basis for processing** (e.g. consent/legitimate interest).

Ensure the **integrity of the data is protected** based on the risk of processing.

## Responsibility

Ensure individuals and processing systems have **defined and documented** responsibilities and appropriate authorisation levels.

Ensure policies are shared with and approved at **strategic and/or board level**.

Ensure **all processing activities** are defined and documented.

## Privacy & Data Protection

Ensure **appropriate privacy data is made available** for subject access requests.

Ensure all data collected is **necessary, proportionate and stored** for an appropriate amount of time and in a transparent manner.

Ensure a suitable **data protection policy is available** and published as appropriate.

Ensure there is a **DPIA**.



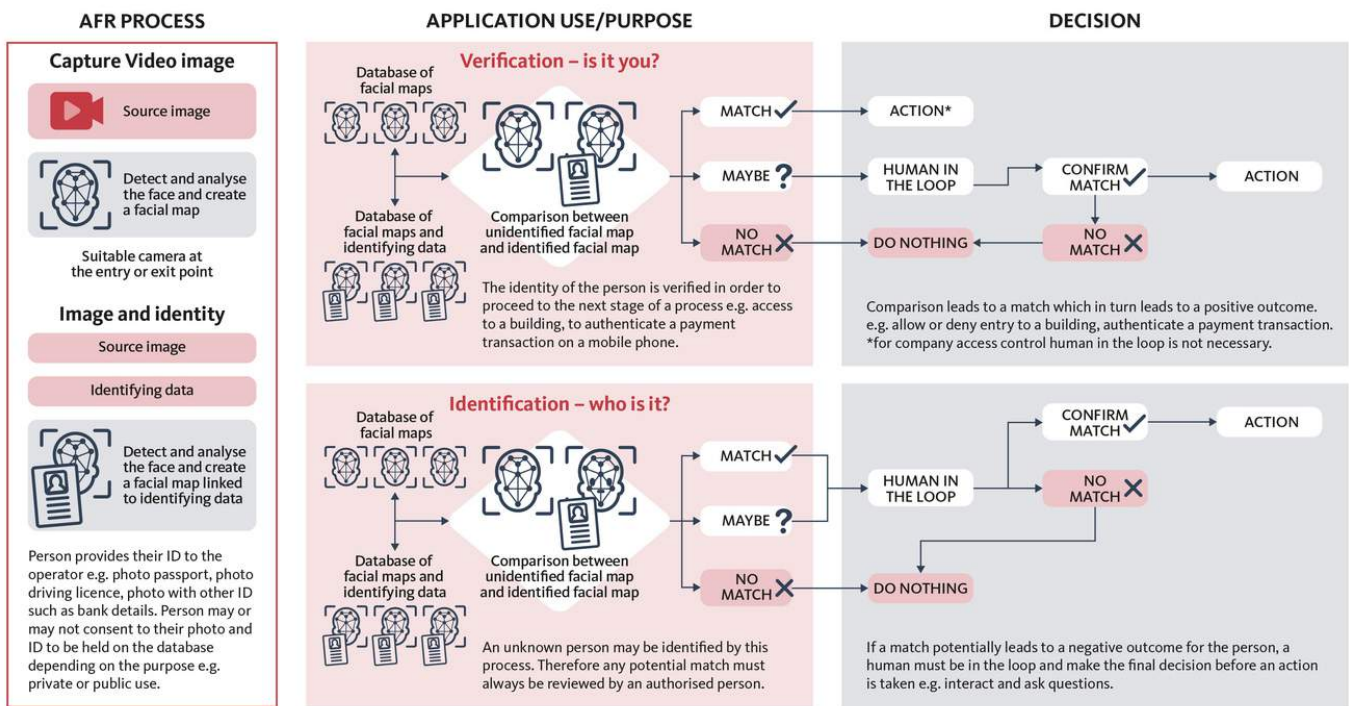


# Operational requirement

The use of biometric technology such as face, voice and fingerprint recognition are fast becoming a part of our everyday lives; many personal devices such as mobile phones and computers use these technologies to provide greater privacy, security and ease of use to access them, and in the same way, such technology is often used to control access (the right to passage) in the private sector business space. But with this technology comes a greater need to ensure those that are impacted by it are made aware of its purpose and that any personal 'data' captured will be used in an ethical way.

AFR systems can be split into two application use themes: for **verification** purposes (e.g. providing access) or for **identification** purposes (e.g. law enforcement). These can be depicted by the following process management summary:

## Automated Facial Recognition / Purpose / Decision



The three key elements of the process management are:

**Capture:** images from individuals are captured by the AFR system and presented to the reference databases to determine any further response.

**Application use/purpose:** dependent on the use of the AFR system, comparison takes place against a database to compare a potential match. Further detail on Verification and Identification applications are explained on pages 12 & 13.

**Decision:** this is the process of deciding whether a face is authenticated by a human for further action or disregarded/deleted.

# Data privacy

Where AFR systems are to be considered, a **DPIA\*** must be carried out to determine the following:

- Identify the need for a **DPIA** (what the system aims to achieve/type of processing involved)
- Describe the processing (collect, use, share, store or delete data)
- Consultation process (how / when to obtain individuals views if/where appropriate)
- Assess necessity and proportionality (lawful basis for processing, can the same objective be achieved by other less intrusive measures?)
- Identify and assess risks (risk of harm to the individual)
- Identify measures to reduce risks (mitigation measures to be used)
- Confirm completion of the **DPIA** and record outcomes
- Integrate outcomes into the **Operational Requirement**
- Keep under review (review the purpose and need regularly)
- Ensure that appropriate signage is in place which warns the public on the use of AFR VSS
- Privacy masking/differential privacy should be utilised when appropriate
- The data controller should be defined

\*An example template of a DPIA can be found on the [Surveillance Camera Commissioner's](#) website.





# Storage & retention

- Consider how long the data is to be kept/retained
- Set out how often the data is to be reviewed
- Data that is no longer needed must be erased and/or anonymised
- The data should be stored securely through physical and electronic security measures
- Data sharing agreements should be in place as appropriate, e.g. between an AFR service provider and a subscriber/user

# Reference database

- Define the purpose of the database in line with ethical and legal requirements
- Define the process required for checking the contents of the database, e.g. deleting poor quality images/replacing with improved quality images, set a retention period/review of interested persons and review risk criteria

**Note:** The quality of images on the database should follow **IEC/ISO 19794-5 - Information technology - biometric data interchange formats, part 5: face image data**

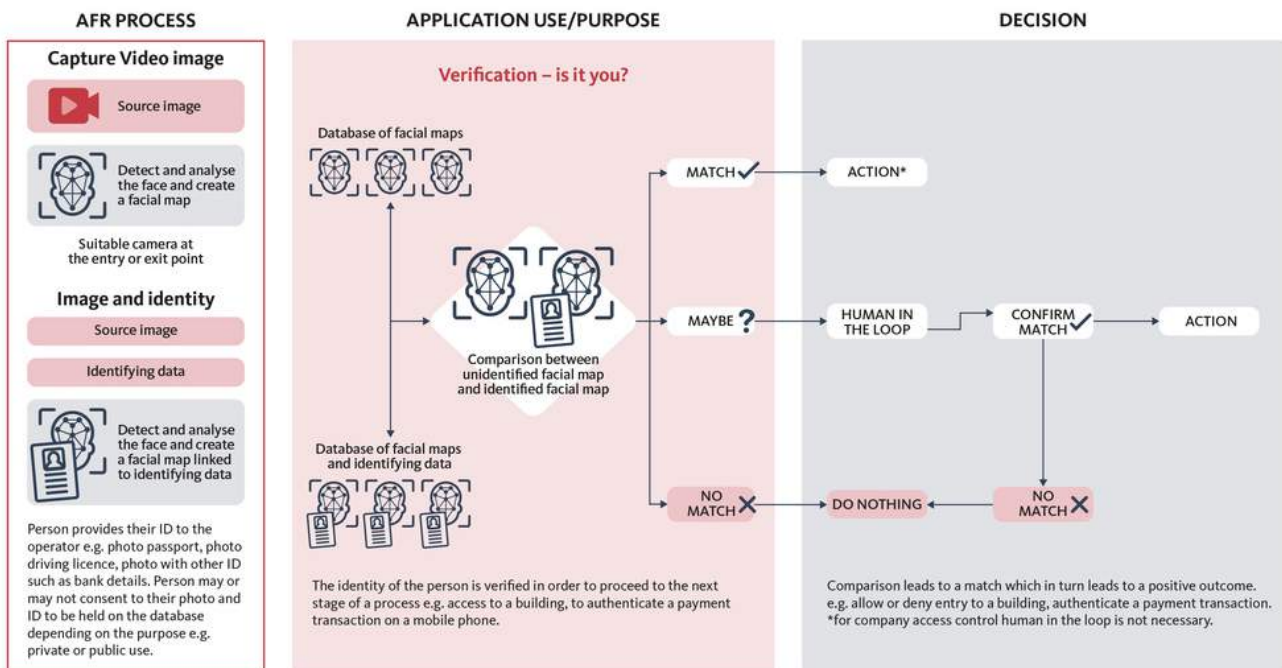
- Where will the database be physically held and is it secure?
  - Ensure that cyber security protections are in place to protect the data
- Note:** Further guidance can be found at the **National Cyber Security Centre (NCSC)**
- Ensure that subject access requests, response times and publication of method to access information is available to the public
  - Consider if images need to be used for evidential purposes, e.g. data validation, image quality, data security etc.



# Verification – is it you?

The use of AFR is divided into two areas: for the purpose of verification, “**is it you?**” and for the purpose of identification, “**who is it?**”.

Where AFR technology is deployed in an organisation for verification purposes, it is important that policies are developed (or existing ones updated) to cover the explanations, considerations and actions that the organisation requires of its employees. Typically, these should cover: **what the rules are, why the rules are in place** and **who the rules apply to**.



## Typical cases for verification

To manage/control the flow of individuals/queuing to meet business service levels and/or to gain authorised access to secure areas

Time and attendance applications to monitor persons of interest for the purposes of payroll and safety purposes i.e. fire evacuation safety, time spent in a specific area, repeat entering of a protected area

Personal access to mobile phones, computers, online banking

Border control/passports to allow the safe and valid passage of persons entering or leaving the country

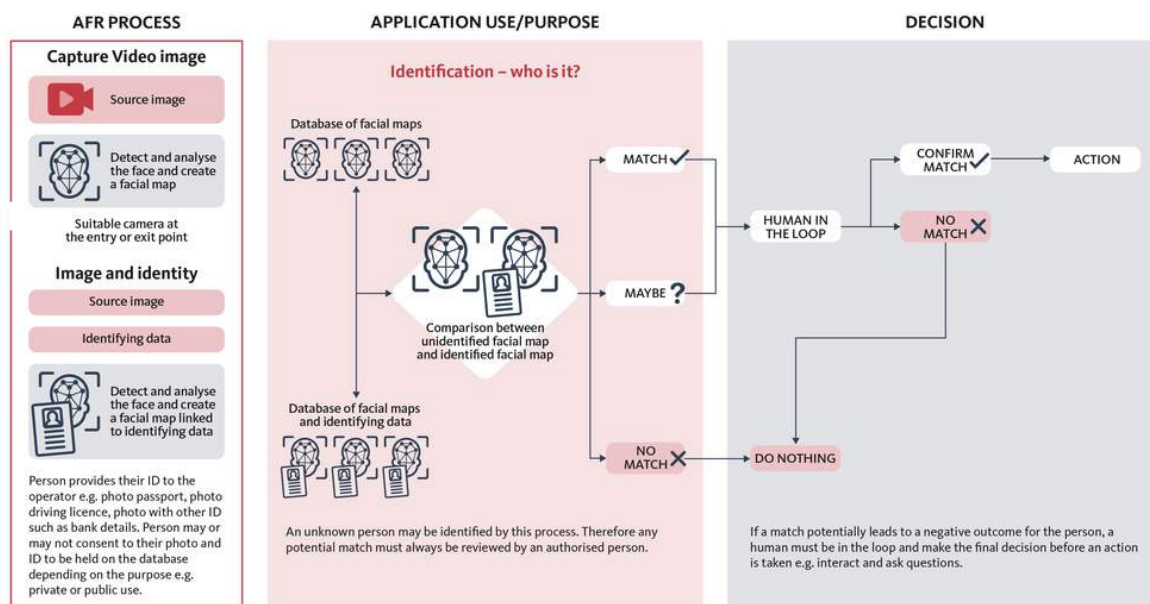


# Identification – who is it?

Where AFR technology is used for identification purposes such as by Law Enforcement\* and other agencies, policies and procedures may take a different form as it may not be appropriate to consult widely with the persons of interest. That does not however mean that such organisations are exempt from the GDPR and Data Protection Act. There will be a need to document persons of interest, whether they are likely to be present at a given time in a monitored location.

It is important that the software does not exhibit any form of bias towards any such persons. It should be made clear that AFR systems where data is stored privately (or by the Government) should be reviewed carefully to ensure they are lawful under GDPR and if held in other locations are legal under the laws for that territory.

\*Commercial (non-law enforcement) and law enforcement often work in partnership (see Surveillance Camera Commissioner Report: Facing the Camera).



## Typical cases for identification

**Border control to identify persons on a known approved watchlist**

**For use in private venues by the owners - shops, museums, stadiums, leisure centres and other private venues where there is a need to control theft or anti-social behaviour**

**For law enforcement purposes to alert to the presence of individuals of interest**

**For private security companies - shopping centres, local authorities to alert to the presence of individuals of interest**

**For law enforcement purposes following VSS footage collected after a notable event or incident**

**Inclusion onto a watch list for the purpose of alerting other business owners of person of interest that may be under suspicion of having committed an offence**



## Useful references

**Biometrics and Forensics Ethics Group: Public-private use of live facial recognition technology: ethical issues**

**Data Protection Act 2018 and the General Data Protection Regulation (GDPR)**

**Data Protection Regulation (GDPR)**

**Equality Act 2010**

**European Human Rights Act**

**ICO: In the picture (V1.2)**

*A data protection code of practice for surveillance cameras and personal information*

**IEC 62676-4:2014: Video surveillance systems for use in security applications**

*Part 4: application guidelines*

**National Institute of Standards and Technology (NIST) - US Department of Commerce (AI Research)**

**Protection of Freedoms Act 2012**

*Part 2: Regulation of surveillance, chapter 1: Regulation of CCTV and other surveillance camera technology*

**Surveillance Camera Commissioner statement - Court of Appeal judgment**

**Surveillance Camera Commissioner report: Facing the Camera**



# About the BSIA

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security.

For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.

*Automated Facial Recognition - a guide to ethical and legal use* is part of the BSIA Artificial Intelligence Series.

The BSIA acknowledge the assistance given by the following member companies in the development of this guide: Anekanta Consulting, Facewatch, JCI, Optex, Secure One and Vigilance.

The BSIA would also like to thank experts for their feedback including Lord Clement-Jones CBE and former Surveillance Camera Commissioner Tony Porter.

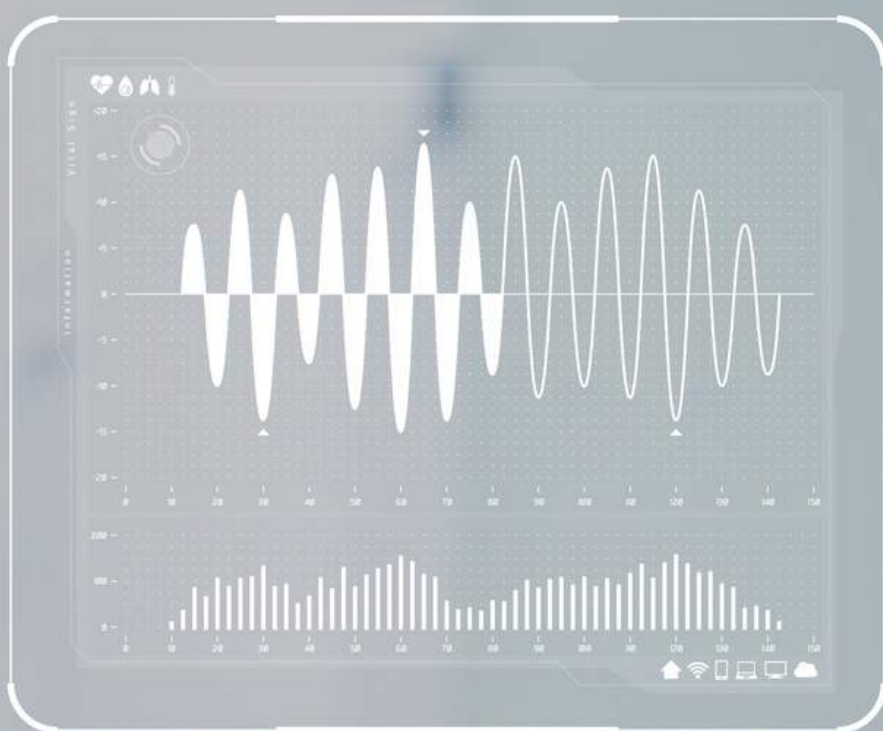
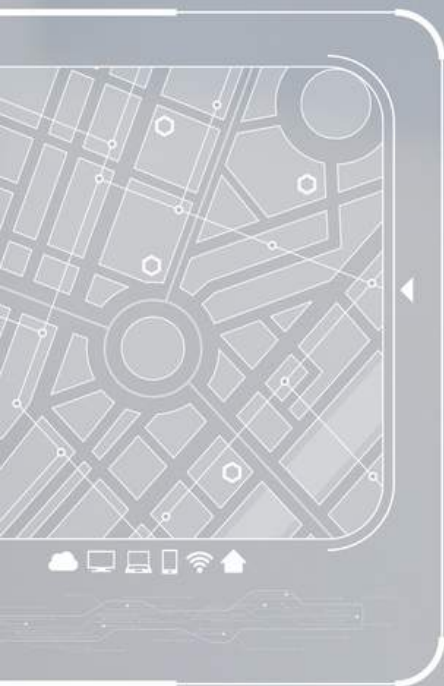
## British Security Industry Association

01905 342020

[info@bsia.co.uk](mailto:info@bsia.co.uk)

[www.bsia.co.uk](http://www.bsia.co.uk)





## *BSIA Artificial Intelligence Series*

**BSIA Form 347 | Issue 1 | January 2021**

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner.