International Standard

ISO/IEC 9868

First edition
2025-02

Information technology — Design, development, use and maintenance of biometric identification systems involving passive capture subjects

Technologies de l'information — Conception, développement, utilisation et maintenance des systèmes d'identification biométriques appliqués sur des sujets de capture passifs

Reference number
ISO/IEC 9868:2025(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Recent improvements in biometric systems, and in particular face recognition, have allowed new usage for identification systems. Biometric systems using artificial intelligence (AI) techniques are capable of capturing biometric data in publicly accessible spaces without any deliberate action from the capture subjects and possibly even without their knowledge.

On 13 March 2024, the European Commission adopted a proposal for a regulation laying down a "uniform legal framework in particular for the development, marketing and use of artificial intelligence".[1] This is one of the first-ever proposed horizontal regulations in the field of AI, aiming at building appropriate standards for safe and human-centric AI systems.

The regulation includes a risk-based framework with a tiered approach. The framework prohibits the use of certain systems posing a particularly high risk to the fundamental rights and safety of individuals, sets out requirements for high-risk AI systems and introduces transparency requirements for other AI systems. The regulation defines high-risk systems, which are systems that pose a risk of harm to the fundamental rights, health or safety of individuals. Biometric identification systems involving passive capture subjects (referred to as "remote biometric identification systems" in the words of the proposal) are classified as high-risk in the regulation risk-based framework. Providers and owners of high-risk systems are expected to demonstrate compliance with European Union (EU) regulatory requirements and identify design/operational risks and mitigation measures before they are put on the European market.

With this development in mind, this document is intended to provide international standardization in a sector which requires strong guidelines and harmonized practices in order to respond to concerns related to privacy protection, bias and accurate performance. It establishes requirements for the design, development, evaluation, operation and maintenance of biometric identification systems involving passive capture subjects.

Many of the examples and use cases found in this document focus on face and face-related biometric systems, given that face biometric characteristics are currently the more commonly used biometric characteristic. Gait and voice are other examples of usable biometric characteristics.

Information technology — Design, development, use and maintenance of biometric identification systems involving passive capture subjects

1 Scope

This document provides recommendations and requirements for the design, development, use and maintenance of biometric identification systems involving passive capture subjects, including pre- and post-deployment evaluation.

While the emphasis is on surveillance systems, this document is also applicable to other types of biometric identification systems involving passive capture subjects, regardless of biometric characteristic or sensing technology. This includes systems involving passive capture of subjects where some capture subjects enrolled voluntarily.

This document does not apply to biometric verification systems and biometric identification systems only involving capture subjects deliberately taking part in the capture.

This document does not define specific services, platforms or tools.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

ISO/IEC 19795-1:2021, *Information technology — Biometric performance testing and reporting — Part 1: Principles and framework*

ISO/IEC 19795-2, *Information technology — Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation*

ISO/IEC 19795-6, *Information technology — Biometric performance testing and reporting — Part 6: Testing methodologies for operational evaluation*

ISO/IEC 19795-10, *Information technology — Biometric performance testing and reporting – Part 10: Quantifying biometric system performance variation across demographic groups*

ISO/IEC 29794-1, *Information technology — Biometric sample quality — Part 1: Framework*

ISO/IEC 30107-3, *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting*

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

ISO/IEC 24745, *Information security, cybersecurity and privacy protection — Biometric information protection*

ISO/IEC 22989, *Information technology — Artificial intelligence — Artificial intelligence concepts and terminology*

ISO/IEC 27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22989 and in ISO/IEC 2382-37 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1 Roles

3.1.1
biometric capture subject
individual who is the subject of a biometric capture process

Note 1 to entry: The individual remains a biometric capture subject only during the biometric capture process.

[SOURCE: ISO/IEC 2382-37:2022, 37.07.03]

3.1.2
biometric system developer
individual or organization that performs development activities (including requirements analysis, design, testing through acceptance) during the system or software life cycle process

Note 1 to entry: While the *biometric system provider* (3.1.3) and biometric system developer can be different entities, all requirements defined in this document for the biometric system developer are under the responsibility of the biometric system provider.

[SOURCE: ISO/IEC 25000:2014, 4.6, modified — Preferred term has been changed from “developer” to “biometric system developer” and Note 1 to entry has been added.]

3.1.3
biometric system provider
natural or legal person, public authority, agency or other body that places a *biometric identification system involving passive capture subjects (BISPCS)* (3.2.1) on the market or puts it into service under its own name or trademark, whether for payment or free of charge

3.1.4
biometric system owner
person or organization with overall accountability for the acquisition, implementation and operation of the biometric system

Note 1 to entry: The biometric system owner is known as the “user” in the EU AI Act.[1]

[SOURCE: ISO/IEC 2382-37:2022, 37.07.09, modified — Note 1 to entry has been added.]

3.1.5
experimenter
individual responsible for defining, designing and analysing the test

[SOURCE: ISO/IEC 19795-1:2021, 3.5]

3.1.6
biometric system operator
person or organization who executes policies and procedures in the administration of a biometric system

Note 1 to entry: In the context of this document, the biometric system operator designates staff from the *biometric system owner* (3.1.4) operating the system

[SOURCE: ISO/IEC 2382-37:2022, 37.07.08, modified — Note 1 to entry has been added.]

3.1.7
passive capture subject
individual who is the subject of a biometric capture process where biometric data capture does not require any deliberate action of biometric presentation by the *biometric capture subject* (3.1.1)

Note 1 to entry: Passive capture subjects are often unaware that their biometric data is being captured and unable to prevent capture.

3.1.8
test crew member
selected biometric data subject whose use of the operational system is controlled or monitored as part of the evaluation

Note 1 to entry: In an operational evaluation, test subjects can be subjects of the operational system or they can be members of a test crew using the system specifically for evaluation purposes.

[SOURCE: ISO/IEC 19795-6:2012, 4.17]

3.2 Categories of biometric identification system and use cases

3.2.1
biometric identification system involving passive capture subjects
BISPCS
biometric identification system where biometric data capture does not require any deliberate action of biometric presentation by the *biometric capture subject* (3.1.1)

EXAMPLE 1 A biometric identification system capturing *passive capture subjects* (3.1.7) walking in a designated area to create biometric probes is a BISPCS.

EXAMPLE 2 A biometric system where biometric capture subjects actively and knowingly participate in the biometric data capture process is not a BISPCS.

EXAMPLE 3 An access control system to a secured building where the personnel have voluntarily enrolled in the biometric reference database is not a BISPCS.

Note 1 to entry: A BISPCS can implement *watchlist identification* (3.2.2).

3.2.2
watchlist identification
process of searching a probe from a *biometric capture subject* (3.1.1) against a biometric reference database to return biometric reference identifier(s) attributable to a biometric person of interest

EXAMPLE A biometric system searching for a missing child in a publicly accessible space.

Note 1 to entry: In watchlist identification scenarios, most biometric capture subjects are not mated to references in the watchlist. Therefore, the expected result is that no reference is returned.

3.2.3
video surveillance system
VSS
system consisting of camera equipment, monitoring and associated equipment for transmission and controlling purposes, which can be necessary for the surveillance of a protected area

[SOURCE: ISO/IEC 30137-1:2024, 3.2.12]

3.3 Miscellaneous

3.3.1
demographic group
category of the human population, defined by specific traits or criteria

EXAMPLE Ethnic group, gender, age group, but also people having facial hair/not having facial hair, wearing make-up/not wearing make-up, wearing accessories/not wearing accessories, etc.

Note 1 to entry: The recognition performance of a biometric identification system can vary across different demographic groups.

3.3.2
manual review
human intervention to achieve a biometric decision

Note 1 to entry: Human intervention can encompass all aspects of a biometric system policy.

3.3.3
monitoring mechanism
mechanism which enables the *biometric system owner* (3.1.4) to assess whether or not the system is functioning as expected

4 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

AI	artificial intelligence
ATM	automated teller machine
BISPCS	biometric identification systems involving passive capture subjects
CAPNIR	concealer attack presentation non-identification rate
CMC	cumulative match characteristic (as defined in ISO/IEC 19795-1)
FND	false negative differential
FNIR	false negative identification rate
FPD	false positive differential
FPIR	false positive identification rate
FRT	face recognition technology
FTAR	failure-to-acquire rate
FTER	failure-to-enrol rate
ML	machine learning
PAD	presentation attack detection
VIP	very important person
VSS	video surveillance system

5 Conformance

Requirements of this document can apply to multiple stakeholders. Some requirements are the responsibility of the biometric system provider. Some requirements are the responsibility of the biometric system owner. Some requirements are the responsibility of both the biometric system provider and biometric system owner. A BISPCS is conformant with this document only if the biometric system provider and the biometric system owner fulfil all their responsibilities.

The biometric system developer can be different from the biometric system provider, but all requirements assigned to the developer are under the responsibility of the biometric system provider.

The biometric system provider, in coordination with the biometric system developer where appropriate, shall document the following:

— the system's intended purpose;

— the rationale for development of the biometric algorithm to process captured data to achieve its intended purpose;

— operating assumptions and limitations;

— types of biometric characteristic to be captured and processed;

— quality and compatibility requirements;

— biometric performance characteristics;

— BISPCS use cases;

— how fitness for purpose for BISPCS use cases is determined.

The biometric system provider can be the same as the biometric system owner, such as a government agency with the resources and skill to train new models using custom internal algorithms.

Biometric system providers and biometric system owners shall fulfil all the responsibilities summarized in Table 1.

Table 1 — Roles and responsibilities

Topic		Role	Representative responsibilities	Applicable Clause/subclause
Risk assessment		Biometric system provider	Assessment for intended use case of the system and provision of suitable mitigation measures	Clause 7
		Biometric system owner	Document assessment for the intended use case	
Design and development		Biometric system provider	Appropriate development of the BISPCS, and testing and validation of all required technical functionalities	Clauses 8 and 9
Operational practice	Competence of biometric system operators	Biometric system provider	Provide training	10.2
		Biometric system owner	Ensure competence is validated	
	Operational security	Biometric system owner	Ensure that the system utilizes appropriately configured and maintained security controls	10.3

Table 1 *(continued)*

Topic		Role	Representative responsibilities	Applicable Clause/subclause
	Privacy measures	Biometric system owner	Review and implement privacy preserving measures	10.4
	Operational monitoring	Biometric system owner	Establish and implement monitoring plan	10.5
	Improvement	Biometric system owner	When necessary, take steps to improve the performance of the BISPCS	10.6

6 Scenarios and use of biometric systems involving passive capture subjects

6.1 Main characteristics

BISPCS have two primary characteristics.

First, a BISPCS interacts with passive capture subjects for whom biometric data capture does not entail any deliberate action of biometric presentation. Capture of biometric data from passive capture subjects is often achieved using biometric capture devices deployed in publicly accessible spaces. The quality of the biometric samples captured from passive capture subjects can be lower than what is usually achieved for cognizant and cooperative presentations and a re-capture step for increasing this quality is not possible.

EXAMPLE 1 Capture subjects are aware while walking down a street that a VSS is capturing their biometric characteristics, but they are not deliberately taking part in a biometric presentation.

EXAMPLE 2 Systems using face recognition in combination with VSS are used in football stadiums for identifying biometric persons of interest as they enter the stadium.

Second, a BISPCS performs biometric identification in which a biometric probe is used to query a biometric reference database to find and return matching reference identifiers. Biometric samples captured from passive capture subjects can be compared against biometric references captured during enrolment, against references captured by another BISPCS, or against references captured by other biometric systems.

6.2 Use cases and scenarios

Examples of use cases and scenarios for BISPCS include:

— search for missing persons;

— protection of public or private spaces;

— watchlist identification;

— investigation after a criminal event.

In the “watchlist identification” use case, the biometric system owner is typically a law enforcement authority but can also be a private entity. In this use case, the biometric reference database contains biometric references of persons of interest together with associated identity or contextual information.

EXAMPLE 1 A VSS uses face, voice or gait recognition to search a watchlist to determine whether people walking in a specific area are persons of interest enrolled in the watchlist.

The watchlist can include biometric references obtained from mug shots, portraits from identity documents, or samples from another BISPCS, like videos or voice recordings. The references can be added to and removed as required while following applicable regulations.

NOTE 1 This type of biometric reference database is referred to as a Type 1 database in A.1.2.

In a typical use case, the BISPCS captures the facial image probes of subjects within range, for example, and compares them against the watchlist to find and return potential matches.

NOTE 2 In some cases, users register voluntarily for a watchlist (e.g. VIP programmes or gambling addicts list in casinos). Such users, as well as all passers-by, are still considered passive biometric capture subjects.

In the "investigation after a criminal event" use case, passive capture subjects can be processed and enrolled in the system to constitute a biometric reference database.

NOTE 3 This type of biometric reference database is referred to as a "Type 2" database in A.1.2.

EXAMPLE 2 A biometric system uses facial recognition to identify whether a suspect was in a specific area at a specified time. Faces from all bystanders present near a crime scene are encoded to constitute the biometric reference database. A biometric probe from a known felon or a suspected felon is then searched against this biometric reference database to determine if they were present.

In this use case, the BISPCS operates at a specific location. The BISPCS can be a VSS which operates routinely for law enforcement purposes or it can be private system.

The biometric probe can be created in various ways, such as from:

— a mug shot, whether pre-existing or acquired during the investigation;

— an available identity document;

— another passive biometric capture, like video recordings.

Further examples of use cases and scenarios can be found in Annex A.

Examples of use cases and scenarios for systems that do not involve passive capture subjects include:

— any biometric systems that verify a biometric claim, such as assessing during border control that a person is the rightful holder of an identity document by comparing a biometric capture with the biometric reference stored in that document, because the system performs a biometric verification and not a biometric identification;

— biometric systems deployed on personal devices, e.g. for unlocking smartphones or biometric validation of remote payment, because the capture subject is actively involved in the biometric capture process;

— biometric access control systems, where persons try to get access to an area by presenting their biometric characteristics to be verified, because the capture subjects are aware of the system and actively involved in the biometric capture process.

6.3 Minimizing identification errors

The quality of biometric data captured from passive capture subjects can often negatively influence identification error rates due to lack of control over capture. As the use cases considered imply that identification errors can lead to adverse consequences for the capture subjects, measures shall be taken to compensate the impact of the false-negative identification rate (FNIR) and the false-positive identification rate (FPIR). These shall include at a minimum:

— the involvement of trained biometric system operators to monitor automated identification results and to adjudicate automated identification decisions;

— a process that utilizes further confirmation that the biometric probe matches a biometric reference when confidence levels of match decisions are low to confirm the true identity of the person in question, e.g. identity document checks.

For some use cases, such as prevention of imminent threats, the BISPCS can process biometric data in real time to raise alerts which are assessed in the field through direct human intervention.

7 Consideration of risk arising from BISPCS

Both the biometric system owner and the biometric system provider shall conduct risk assessment activities. It is recommended that these activities be based on objective criteria and follow references ISO/IEC 31000, ISO/IEC 27701, IEC 31010, ISO/IEC 29134, ISO/IEC 23894 and ISO/IEC 42001.

The biometric system provider shall conduct a risk assessment based on the intended use cases of the system and provide suitable mitigation measures for its operational deployment. The biometric system provider shall provide clear and understandable information and documentation to the biometric system owner about the intended use case, capabilities and limitations of the system and any other factors that can affect risks.

The biometric system owner shall assess the risks that the BISPCS can pose in the specific use case and target environment, including whether BISPCS is the most appropriate technology for the intended purpose. The biometric system provider should assist the biometric system owner in this use-case-specific risk assessment. Given the socio-technical nature of risks – in that such risks concern the interaction of the technical capabilities and limitations of a system, with social, legal, regulatory and environmental factors specific to the context in which a system is deployed – this use-case-specific risk assessment is important.

Biometric system owners shall produce a risk assessment document in which the consequences of the following kinds of error are discussed:

— a false negative, where the capture subject is in the reference biometric database but no identity is returned;

— a false positive, where the capture subject is not in the reference biometric database but another identity is returned;

— a false positive, where the capture subject is in the reference biometric database but another identity is returned;

— a failure to acquire, where a biometric sample should be captured, but is not.

The biometric system owner can incorporate developer-provided information into this risk assessment.

The following examples show potential considerations which can arise in a risk assessment for a theoretical use case.

EXAMPLE 1 In a “compulsive gambler detection” use case, a missed detection or a false negative can allow a compulsive gambler into the casino, while a false positive can lead to an incorrect inquiry or expulsion of a legitimate casino patron.

EXAMPLE 2 The developer’s recognition algorithm documentation describes elevated false positive rates in children. In the compulsive gambler detection use case, this is immaterial because policy is not to enrol children.

EXAMPLE 3 The developer’s recognition algorithm documentation indicates the highest false positive rates in individuals exhibiting certain racial and ethnic features. The threshold has been set to achieve the desired false positive rate data on that population, so it is anticipated that the overall false positive rates will be lower than that specific rate.

NOTE Risk assessments can be made in conjunction with external stakeholders and special interest groups, including but not limited to civil liberties, policy equity, legal advocacy and justice organizations.

For the specific use case of facial recognition used for law enforcement, the World Economic Forum published a white paper on responsible use.[8] In the absence of local regulation and before deploying a BISPCS, a biometric system owner can use the proposed self-assessment questionnaire in Reference [8] to ensure that they have introduced appropriate risk-mitigation processes.

8 Design and development practice

8.1 Biometric system and algorithm

The biometric system developer shall document the system's intended purpose, and the rationale for developing the biometric algorithm to process captured data to achieve this intended purpose. The biometric system developer shall also document operating assumptions and limitations, types of biometric characteristic to be captured and processed, quality and compatibility requirements and biometric performance characteristics. The biometric system developer shall document the BISPCS use cases and how fitness for purpose for these is determined.

The biometric system developer should utilize controls described in ISO/IEC 42001. Organizations can implement these controls to assure that the BISPCS considers impacts to interested parties, to design and develop AI responsibly, and to assure the use of high quality data.

For developing a VSS, see ISO/IEC 30137-1 for further information.

The biometric system developer should aim for the biometric algorithm to reach sufficient biometric performance according to the use case, such as FNIR/FPIR trade-off for the target FPIR operating point. Biometric performance measurement during development shall be documented using relevant testing and reporting methodologies defined in ISO/IEC 19795-1, ISO/IEC 19795-2 and ISO/IEC 19795-10. Biometric algorithm performance shall be based on training, validation and testing datasets consistent with the intended use case which is provided by the biometric system owner. The biometric system provider shall document compliance with applicable data protection requirements.

The biometric system developer shall work to minimize differential recognition error rates across demographic groups comprising the target capture subjects for the system. The biometric system developer shall document efforts to reach sufficient biometric performance and to reduce demographic differential of error rates. Such documentation shall include information on biometric algorithm development as well as the training and selection of a machine learning model.

Biometric performance testing documentation shall state the degree to which biometric algorithm performance is sufficient and fit for the system's intended purpose.

EXAMPLE 1 The biometric performance testing report specifies the sample quality and resolution necessary for the biometric algorithm to achieve a specified level of performance. This is information that biometric system owners can then use.

The training and validation datasets should include data representative of the intended use case, including environment and target population. The training and validation datasets may additionally include more diverse data and the balance between groups may be different than the target population for generalization purposes. The use of training and validation data shall be consistent with any licence or user-generated content restrictions.

As far as possible, the testing dataset shall be representative of the target population and the intended use case, and the test reports shall describe the efforts taken to achieve this objective. This is necessary to predict the performance of the deployed system, including the projected performance differential for different demographic groups. The report should provide data on differential performance across demographic groups so that stakeholders can determine whether performance is in line with the general principles of fairness and non-discrimination of all individuals.

Training and testing datasets shall be disjoint sets.

EXAMPLE 2 The report before release of a system can include biometric performance reported on various demographic groups representative of the target population with empirical validation of a low differential.

The biometric system developer should embed mechanisms to provide explainability of the BISPCS outputs to the biometric system operator.

NOTE ISO/IEC TS 6254:—[1)] intends to provide support for development of such mechanisms.

1) Under preparation. Stage at the time of publication: ISO/IEC DTS 6254:2025.

The BISPCS should be developed so that comparison scores returned are understandable by a biometric system operator. Preferably, the comparison score should be directly interpretable as an expected FPIR and this interpretation should be stable throughout the system life cycle (for example, to automatically compensate for changes such as increase of biometric reference database size or to the environment).

EXAMPLE 3 For a given system, an increase of 10 in comparison score is interpretable as a tenfold decrease in expected FPIR. Therefore, for example, if a comparison score of 10 corresponds to 1 % FPIR, then a comparison score of 20 corresponds to 0.1 % FPIR and a comparison score of 30 corresponds to 0.01 % FPIR.

8.2 Impact of capture devices on training and testing

Biometric developers should select training data from relevant capture devices that is representative of operational use. For systems that utilize a specific biometric algorithm for a particular capture device, the developer should train machine learning models on data from all relevant variations of the capture device.

If biometric capture devices have various settings in order to be adapted to various acquisition environments, samples acquired using these various settings should be included in the training data.

To assess the performance of the system, the testing dataset shall include data from biometric capture devices representative of the intended use case with settings corresponding to the intended acquisition environment. For systems that deploy a biometric algorithm which is not specific to a particular capture device, that algorithm should be capable of performing effectively against samples from a broad variety of biometric capture devices.

The BISPCS shall implement a method to quantify the quality of the biometric samples in accordance with ISO/IEC 29794-1. However, unlike the case of a biometric identification system involving capture subjects deliberately taking part in the capture, this quality assessment cannot be used in feedback loops with the capture subjects to improve a presentation and meet specific quality requirements. Similarly, depending on the implementation, it is typically not possible to initiate a new capture if quality is too low. Implementations with multiple capture devices can have several opportunities to capture a subject, using continuous quality assessment to select the highest-quality sample.

NOTE For a BISPCS implementing speech recognition, Reference [10] can be used as a reference to assess quality.

The quality assessment should be used to define thresholds after which samples are deemed to be of insufficient quality for manual review (and are thus discarded) or to highlight possible defects to be reported to the biometric examiners so they can choose to consider or reject the candidate.

EXAMPLE 1 A face recognition system returns a candidate based on a face portrait with a low inter-eye distance. The biometric examiner can choose to discard the candidate as the resolution is insufficient for manual review.

The biometric capture devices and any supplemental illumination should be selected and configured to support capturing subjects in motion in the intended environment.

EXAMPLE 2 For subjects running, sensor integration time is short to avoid motion blur.

9 Technical capabilities of the system

9.1 Performance

9.1.1 General

Before releasing a BISPCS, the biometric system provider shall test the system to ensure that it behaves according to specification, with special attention to error rates.

9.1.2 Biometric recognition

The evaluation of the performance of a BISPCS shall consider the recommendations and conform to the requirements of ISO/IEC 19795-1 regarding the testing and reporting of identification systems. The performance metrics reported shall be as defined in ISO/IEC 19795-1:2021, 12.7.

The evaluation of the performance of the system shall be conducted in an environment which is representative of the intended operational environment. The test report shall describe the scenario, including environmental conditions, demographic groups of the test subjects, size of the biometric reference database, desired setting for FPIR and FNIR, and considerations on a possible trade-off between speed and performance.

For systems returning a list of candidates, the CMC curve should be plotted as described in ISO/IEC 19795-1.

Special care should be taken to ensure statistical relevance of FPIR evaluation and the Rule of 30 should be followed as defined in ISO/IEC 19795-1:2021, Annex B.

9.1.3 Demographic differential performance assessment

The biometric system provider should assess the performance of the system false negative and false positive identification rates across different demographic groups using appropriate established performance requirements.

When evaluating the demographic differential performance of a BISPCS, an experimenter should consider the recommendations and conform to the requirements of ISO/IEC 19795-10. The experimenter of the system shall use suitable demographic differential metrics in ISO/IEC 19795-10 based on the precise use-case of the system under evaluation. The choice of demographic differential metrics should be properly justified in the test report.

9.1.4 Detection of anomalous image quality

The BISPCS shall implement biometric sample quality evaluation mechanisms as discussed in 8.2. In particular, these mechanisms shall be used to monitor if biometric sample quality statistics as observed in operational deployment significantly differ from the statistics measured with the datasets used to train and test the system during development.

In order to assess robustness of the system, the biometric system provider shall describe efforts made to have a test dataset with biometric sample quality representative of those observed in operational deployment.

EXAMPLE For a face biometric characteristic based system, the test dataset includes a proportion of samples for which the capture subjects wear medical masks representative of real deployment to assess the robustness to facial occlusions.

9.1.5 Security evaluation and presentation attack detection

While bona fide capture subjects of a BISPCS do not deliberately take part in the biometric capture, some individuals can actively seek to avoid recognition by concealing their biometric characteristics.

EXAMPLE An attacker can wear glasses or make-up to hide or change their facial biometric characteristic or parts of it, in order to avoid recognition.

Depending on the security objectives, a biometric identification system involving passive capture subjects can deploy concealer presentation attack detection mechanisms.

If presentation attack detection mechanisms are implemented by a BISPCS and are relevant for operational use case, they shall be evaluated by the biometric system provider following the requirements of ISO/IEC 30107-3 applicable for testing and reporting of identification systems.

In case of security sensitive applications, a security evaluation can be relevant. In this case, the security evaluation should be conducted following the principles of ISO/IEC 19792 and the ISO/IEC 19989 series.

9.1.6 Third-party ex-ante performance evaluation

BISPCS performance should be assessed ex ante, i.e. before deployment, by an independent third party in order to provide assurance of the evaluation.

Ex-ante performance evaluations shall be based on ISO/IEC 19795-1, ISO/IEC 19795-2 and ISO/IEC 19795-10.

Mechanisms should be in place to generate an evaluation report on the performance of a BISPCS (including accuracy, throughput and differential performance across demographic groups as defined in ISO/IEC 19795-10) and to communicate results to an independent auditor for the assessment of the claims of the biometric system provider.

Where possible, the third party should perform a scenario evaluation of the BISPCS before deployment, following methodologies defined in ISO/IEC 19795-2.

If presentation attack detection mechanisms are employed by the system, the third party shall evaluate them in accordance with the requirements of ISO/IEC 30107-3 applicable for testing and reporting of identification systems.

The biometric system provider or the third-party evaluator should generate an audit report that states each piece of information given in Annex B or a paragraph of text explaining why it is absent.

9.2 Security and integrity

The BISPCS shall be developed and deployed in a secure fashion.

The security objectives depend on the intended use of the biometric identification system under consideration.

When operating the biometric system, security controls shall be implemented to:

— mitigate the risk of unauthorized access, use, modification, deletion and disclosure of biometric data;

— mitigate the risk of data poisoning, i.e. ensure that training data have not been contaminated with data that can cause undesirable outcomes;

— protect the integrity of system data including log data;

— limit administrator and biometric system operator access to system data to authorized persons, based on the principle of least privilege.

The BISPCS shall implement confidentiality and integrity measures following the principles of ISO/IEC 27001 and ISO/IEC 24745, especially for the biometric reference database.

The cybersecurity of the system shall be ensured to mitigate the risks of alteration of the functions of the system, by using the appropriate controls from ISO/IEC 27002, following the principles of ISO/IEC 27001. Technical and process controls shall be implemented to mitigate the risk of modification of the biometric reference database by an attacker.

The biometric system provider should implement as many security controls as reasonable given the intended use to ensure the system is secure by design before being deployed, operated, or both, by the biometric system owner. The biometric system provider should explicitly document what remains to be implemented by the biometric system owner.

The biometric system provider shall conduct a comprehensive risk assessment following ISO/IEC 27005 to manage residual risks and confirm appropriateness of security controls.

To check the integrity and trustworthiness of the remote subsystem such as capture devices, the technology in ISO/IEC 24761 may be applied (see ISO/IEC 24761:2019, 5.2.3.3).

9.3 Biometric data management

The BISPCS shall be developed and deployed in a way that affords sensitive data protection, as appropriate, including deletion strategies.

Biometric enrolment data records should be present in the biometric reference database only for a duration appropriate for the application's intended use. Policies shall be established and maintained that require biometric system owners to remove identifiers and delete linked biometric references when data retention

is no longer justified. Automatic notification at regular intervals can be implemented so that the system administrator can validate if a given identifier needs to be kept in the biometric reference database.

When enrolling a new entry in the system, the BISPCS shall provide feedback regarding the quality of biometric characteristics to allow biometric system operators to evaluate this new input data, based on ISO/IEC 29794-1. Systems should offer the possibility to link multiple biometric samples (e.g. multiple images of the same person's face) to a single identity to reinforce the accuracy of the matching.

During enrolment, a deduplication check should be automatically performed to check if the capture subject is already in the biometric reference database, and the biometric system operator should have the option to fuse with an existing identity or create a new one as appropriate. All decisions by the biometric system operator shall be logged.

The BISPCS should be capable of setting an automatic deletion date when enrolling a new subject into the watchlist.

9.4 Support for manual review

The BISPCS shall include processes ensuring the automated match/non-match decisions produced by the system can be reviewed manually by individuals trained for the task.

EXAMPLE 1 In face examination, the individual is specifically trained to not over-favour automatic decision (automation bias) or to not favour their own belief when interpreting the output of the system (confirmation bias).

The BISPCS workflow should support the following:

— side by side manual review of probe and reference biometric samples;

— ability to categorize the decision:

  — confirmed,

  — rejected,

  — uncertain;

— ability to indicate to biometric system operators that the probe or reference biometric samples from the biometric reference database has been processed (e.g. enhanced, cropped);

— ability for manual review of original sources (i.e. before any image processing like detection or cropping operations).

Systems shall provide the capability for multiple biometric system operators to independently perform manual reviews of automated match/non-match decisions in a “double blind” fashion: in this workflow, biometric system operators do not know which other biometric system operators are working on the same decision or what their conclusions are.

EXAMPLE 2 For a criminal investigation, two face experts independently perform manual reviews of the same event without collaboration before returning their decisions to the investigators. The event is considered confirmed only if both decisions are in agreement.

NOTE A system policy that has been defined and documented by the biometric system owner determines how the final decision is managed when manual reviewers do not have the same assessment of the comparison. A possible policy is to have a third opinion if two manual reviews do not agree. Another policy could be to conclude to a no match as soon as at least one manual review assessment is no match.

Mechanisms shall be in place to reduce external influences on biometric system operator decision-making. In the case of a criminal investigation, the system should allow for a manual review of the evidence with limited background information. In particular, the manual reviewer should not be informed of the context of the investigation.

EXAMPLE 3 In criminal investigation, the manual reviewer is not involved in the case so as not to prejudice the manual review process or affect the manual reviewer’s objectivity

The system shall log all human decisions and outcomes. All images from manual reviews shall be stored and kept as part of the systems audit.

Best practice is to not make any changes to the BISPCS until manual reviews have been completed. If an enrolment results in an alert requiring manual review, the BISPCS shall record all post-manual review decision actions, such as unenrolment events.

9.5 Support for human oversight

The BISPCS shall include logging capabilities enabling the recording of relevant events. The BISPCS shall include audit trails and dashboards to monitor system behaviours and biometric system operator actions. These approaches ensure that BISPCS activities and data are accurately traced over the duration of the life cycle of the system. The logging of the events should ensure traceability of the BISPCS that is appropriate to the intended purpose of the system.

The system shall implement integrity protection mechanisms to ensure that audit trails cannot be tampered with undetected. This can for example be achieved by using digital signature on the audit trails to ensure their authenticity and integrity.

Data access authorisation shall be clearly defined based on users access and roles in the system to ensure only the authorized persons have access to specific functions. The BISPCS shall implement secure authentication mechanisms that can restrict access to data, information, tools and functionality based on roles and responsibilities (such as administrators and biometric system operators).

9.6 Support for operational testing

The biometric system provider shall provide mechanisms to enable the assessment of the operational performance of the system.

The mechanisms used to support testing activities shall include processes to add and remove references or probes in the system in order to perform mated and non-mated transactions.

EXAMPLE For evaluation of a watchlist scenario non-mated transactions can be performed by acquiring samples from a test crew member and comparing them to the watchlist, after ensuring that the operational watchlist does not include test crew members.

9.7 Documentation

The biometric system provider shall provide documentation on system capabilities and limitations, including instructions for proper use by the biometric system owner. The documentation should also include the impact of environmental factors on the biometric recognition performance of the system to guide responsible deployment.

The biometric system provider can provide different documentations for different target readers. Inclusion of technical details whose disclosure can affect the security of the system should be done on a need-to-know basis.

Documentation intended for a third-party experimenter may describe some features of the system with more technical details than necessary for the biometric system owner to operate the system.

EXAMPLE Documentation intended for an evaluation laboratory includes details of any presentation attack detection mechanisms included in the system, to facilitate their testing.

Documentation shall include all information required to:

— identify the system, such as version number or biometric system provider identifier;

— install and operate the system, such as hardware and environment requirement.

In particular, with regards to the content of this document, documentation shall cover:

— information from reports made during development, as described in 8.1, such as description of testing datasets, performance evaluation as described in 9.1 and intended purpose of the system as described in Clause 7;

— requirements on minimal quality for biometric samples obtained from capture devices as described in 8.2;

— details of all implemented features supporting human interaction processes and manual review as discussed in 9.4;

— recommended policy from the biometric system provider regarding machine learning model retraining, as discussed in 10.6.1;

— details of all implemented features supporting operational monitoring mechanisms discussed in 9.5;

— mechanisms supporting operational testing as discussed in 9.6.

10 Operational practice

10.1 Organizational control

The biometric system owner should utilize controls described in ISO/IEC 42001. Organizations can implement these controls to assure that the BISPCS is deployed, operated and maintained appropriately.

10.2 Competence of biometric system operators

It is the responsibility of the biometric system owner to ensure that its biometric system operators are able to effectively operate and act on the output of a system in a way appropriate for risks identified in the risk assessment.

Biometric system owners shall validate that biometric system operators are assessed as having a comprehensive knowledge of the capacities and limitations of the biometric systems they operate. This process of competence validation should be renewed regularly and in particular when the system has a major update.

The biometric system provider, in conjunction with the biometric system owner and other qualifying entities, as appropriate, should offer training services so that biometric system operators from the biometric system owner are properly trained.

As proposed in Reference [8], this training should include:

— knowledge of and updates of possible mandatory regulations, laws or policies affecting the operation of the BISPCS;

— awareness of the risk of biases (training to understand potential difference performance for different demographic groups, particularly false positive and false negative identification rates; knowledge of how to calibrate and adjust the threshold of the system; understanding of how to configure the system in the manner appropriate to the specific circumstances and risks of a given use case, and how to set the length of the candidate lists for manual review);

— understanding of the risk of false negative and false positive errors (overestimation of own capability, risk of over-reliance on technology, blind spots, risk of human bias such as other-race effect bias);

— awareness of the risk of false positives from twins, siblings and other related individuals;

— awareness of the risk of image manipulation, including data integrity attacks and data morphs, and the tools to identify them;

— ethical awareness (identifying the presence of vulnerable data subjects or areas frequented by vulnerable data subjects, such as schools, playgrounds, hospitals and places of worship);

— how to use tools that assist examiners in understanding the reasoning behind systems' decisions and recommendations.

10.3 Operational security

The biometric system owner shall ensure that the system as deployed utilizes security controls that are configured and maintained appropriately.

The biometric system owner shall conduct a comprehensive risk assessment following ISO/IEC 27005 to manage residual risks and confirm appropriateness of security controls.

10.4 Privacy measures

10.4.1 General

The biometric system owner shall review privacy-preserving measures following the principles of ISO/IEC 29100 and ISO/IEC 24745, implement such measures as appropriate, and ensure that the BISPCS follows applicable privacy laws and regulations.

10.4.2 Privacy principles of ISO/IEC 29100

10.4.2.1 Summary of privacy principles

The privacy principles of ISO/IEC 29100 are summarized in ISO/IEC 29100:2024, Table 3. In the context of this document, the following apply:

1) consent and choice;
2) collection limitation;
3) data minimization;
4) use, retention and disclosure limitation;
5) accuracy and quality;
6) openness, transparency and notice;
7) individual participation and access;
8) accountability;
9) information security;
10) privacy compliance.

10.4.2.2 Consent and choice

NOTE The ISO/IEC 29100 privacy principle "consent and choice" is usually not met in BISPCS and strict adherence is not always possible.

The BISPCS target passive capture of biometric data by design, and so consent is out of scope for this type of data collection. Public awareness helps mitigate privacy risk; see 10.4.2.7.

When biometric capture subjects are made aware of the capture by a BISPCS, they should be informed of how and for what purpose their biometric information will be used, as discussed in 10.4.2.7.

Capture subjects are usually not solicited to consent to the use of their biometric information for identification purposes in a BISPCS and can only avoid having their biometric information captured if they are aware of the BISPCS and leave the area before their biometric data is captured.

10.4.2.3 Collection limitation

Adhering to the collection limitation principle means limiting the collection of personally identifiable information to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s). This aspect is particularly important during the enrolment phase when biometric data used for identification purposes in a BISPCS is collected.

The biometric system owner shall ensure that the data collected by the BISPCS is limited to what is necessary in relation to the purposes for which it is processed.

10.4.2.4 Data minimization

While in storage, biometric references shall be protected from unauthorized disclosure. Protective measures can include data encryption, access control and renewable biometric references. For further information see ISO/IEC 24745:2022, Clause 8.

In addition to biometric reference data, the collection and retention of other identity-related attributes shall be minimized. The inclusion of any identifying attributes shall be justified by the context of use of the system. When the identity-related attributes need to be stored, they should be protected using de-identification techniques following ISO/IEC 20889 and ISO/IEC 27559 to the maximum level of de-identification that is compatible with the context of use.

10.4.2.5 Use, retention and disclosure limitation

The biometric system owner shall limit the use of biometric data collected in accordance with the legal constraints of the jurisdiction in which the data are collected and relevant system policy.

Biometric references shall be deleted when retention is no longer justified. Based on the use case, biometric references deletion can happen as soon as the biometric capture subject is not identified in the biometric reference database. Justifications for retention include:

— timeframe for the purpose of its processing has not expired;

— legal retention requirements (for some use cases, retaining probe data can be legally required to improve the oversight and auditability of the system and confirm that probe transactions were following the system policy);

— reasonable practicality issues (e.g. data are kept in the system until the next planned review of the dataset).

The biometric system owner shall constrain the disclosure of biometric data collected in accordance with the legal constraints of the jurisdiction in which the data is collected as well as relevant cross-jurisdiction constraints (e.g. domestic and international). When the biometric reference database is transferred internationally, the biometric system owner should be cognizant of any additional national or local requirements specific to cross-border transfers.

10.4.2.6 Accuracy and quality

The biometric system owner shall ensure that the identifying biometric and non-biometric data collected for an individual is accurate and of sufficient quality. The biometric system owner shall ensure the biometric and non-biometric data is appropriate for its intended use and disclosure (i.e. it is complete, up-to-date).

This principle is particularly important in cases where the BISPCS is used to grant or deny a significant benefit to an individual or where data lacking accuracy or quality would result in significant harm to an individual.

10.4.2.7 Openness, transparency and notice

As appropriate, the biometric system owner shall include in notices an open, transparent declaration of the purpose for which the biometric reference database set will be processed.

In accordance with relevant jurisdictional legislation, the biometric system owner shall provide information in a reasonably accessible manner that informs the public about the system in use. This can include:

— intended function of the system;

— how the system works;

— the biometric modality in use;

— the provider of system;

— the means of individual participation and access.

This information can, for example, be displayed as informative text on posters. The information should include a URL or QR encoded URL for a website containing the required information.

There can be explicit signage notifying capture subjects when they are entering an area where a BISPCS is operating. This can, for example, include physical marking on the ground or walls or both.

EXAMPLE 1 The use of a VSS system is shown transparently in publicly accessible spaces and it specifies that biometric data are also being captured and potentially analysed.

NOTE 1 This public awareness can follow national data protection guidance where appropriate.

Transparency and public awareness can mitigate many of the possible risks of BISPCS, for example by making individuals aware of the use case and allowing them to take action to object to it if necessary.

EXAMPLE 2 In a gambling addict watchlist, enrolled individuals can update their reference data as well as request the deletion of biometric probe data captured by the BISPCS.

NOTE 2 Transparency encourages organizations to consider their purposes carefully. In many countries, transparency is also a legal requirement for data protection.

Biometric algorithm testing documentation as described in 8.1 can be made public where appropriate. The content should balance the need for transparency with the need for intellectual property protection and system security, in accordance with applicable guidance or regulations.

10.4.2.8 Individual participation and access

The biometric system owner shall allow each individual to access and review their reference data, provided their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law.

Individuals should be able to update their reference data, or request their reference data be deleted if not prohibited by applicable law, since reference aging can mean that such data no longer accurately represent the natural person concerned.

NOTE 1 For some use cases, like watchlist for law enforcement, capture subjects are not willingly enrolled in the system. Therefore, the ability to review or update their data is not applicable.

NOTE 2 For a missing person watchlist use case, the update can be performed by relatives, or by the person in watchlist if the inclusion was inappropriate.

10.4.2.9 Accountability

The biometric system owner should follow the measures described in ISO/IEC 29100:2024, 6.10. When this is not possible, explanations should be provided in the documentation of the BISPCS.

10.4.2.10 Information security

The biometric system owner should follow the measures described in ISO/IEC 29100:2024, 6.11. When this is not possible, explanations should be provided in the documentation of the BISPCS.

10.4.2.11 Privacy compliance

The biometric system owner should follow the measures described in ISO/IEC 29100:2024, 6.12. When this is not possible, explanations should be provided in the documentation of the BISPCS.

10.4.3 Biometric information protection

The system should implement measures to ensure the protection of integrity and confidentiality of biometric data and associated identification data stored and processed by the system. See ISO/IEC 24745 and ISO/IEC 30136 or further information.

If applicable for the specific use case of the BISPCS, biometric reference data should be protected to ensure irreversibility, unlinkability and renewability, and the following apply:

— the biometric system provider should rely on one of the models described in ISO/IEC 24745:2022, Clause 8, to enable the biometric system owner to store renewable biometric references;

— additionally, the level of confidence on the privacy measures applied to biometric data shall be assessed and documented. ISO/IEC 30136 metrics and methodology can be used to report to which extent the system ensures irreversibility, unlinkability and/or renewability.

10.5 Operational monitoring

10.5.1 Monitoring

A monitoring plan shall be established and implemented by the biometric system owner to assess whether the system is functioning as expected. The biometric system provider should assist the biometric system owner in the creation and execution of the plan. This operational monitoring shall be done by way of audit logs, reports and monitoring of biometric system operators, administrators and actions in the system, as described in 9.5.

This monitoring plan shall include an internal audit, as described in 10.5.2, planned on a regular basis.

If changes occur to operational system hardware (e.g. capture devices) or software (e.g. biometric recognition algorithms, PAD detection techniques), monitoring and auditing procedures and associated data shall be reviewed and updated as necessary.

10.5.2 Operational testing and internal audit

As described in 9.1, the biometric system provider is responsible for appropriate testing to demonstrate acceptable projected performance before deployment. Once the system is in operation, the biometric system owner shall perform operational testing to assess whether system is performing in a manner that is fair, safe and reliable for the relevant use case, in line with the instructions from the documentation.

The biometric system owner, using mechanisms discussed in 9.6 should assess the performance of the system on a regular basis to assure consistency of operation after initial deployment, as planned in the monitoring plan described in 10.5.1.

The biometric system owner shall report to the biometric system provider any serious incident or risk identified. The biometric system provider should assist the biometric system owner, or the biometric system owner can evaluate independently, in line with the instructions from the documentation.

The test plan shall conform to the requirements of ISO/IEC 19795-6 on operational evaluation and shall be adapted to the use-case evaluated.

The test plan shall define the benchmark values for relevant performance metrics to be achieved by the system appropriate for the operational need.

Operational testing shall involve the use of a test crew, as defined in ISO/IEC 19795-6. To measure the FPIR and FNIR during operation, it is necessary to establish the ground truth against which identification

decisions made by the system can be compared. The process to establish ground truth should follow ISO/IEC 19795-6.

Where manual adjudication of matching decisions is employed in operational use, FPIR and FNIR can be based on automated system decisions or on manually-adjudicated decisions. To simulate behaviour of passive capture subjects, the test crew should be habituated to the collection environment in a fashion consistent with typical use.

EXAMPLE 1 During an operational evaluation of a system using VSS capture devices, the test crew is not informed of the positioning of the capture devices and instructed not to try to localize them.

EXAMPLE 2 The test crew is emulating daily commuters who follow a regular walking path through a space.

EXAMPLE 3 A VSS is set up in a plaza where the test crew is emulating tourists standing and looking in various direction.

In the case of any biometric algorithm update, such as machine learning model retraining, or change in biometric capture device, the biometric system owner shall assess the performance of the system to assure consistency or gain in effectiveness of operation in a manner which is logistically and practically feasible.

As the size of the operational biometric reference database affects the passive biometric system accuracy, the biometric system owner shall have a defined test plan policy to assess regularly that FPIR remains at a desired value.

In case of a change of the biometric capture device, if operational performance has been adversely affected, appropriate changes shall be made to restore the performance to acceptable levels, as discussed in 10.6.3. Retraining can be called for if a regression of performance is observed. See 10.6.1 for further information.

The internal audit should produce an evaluation report on a regular basis, including, for example, differential performance, as defined in ISO/IEC 19795-10. This report should include statistics on identification transactions, such as number of candidates returned for a time period, which should be properly analysed in order to detect potential defective functioning.

EXAMPLE 4 An increase in FNIR in an operational site can indicate a capture device quality issue.

NOTE The internal report can be submitted to relevant market surveillance authorities, for example on an annual basis.

10.5.3 Feedback

The biometric system provider should implement mechanisms that allow the biometric system owner or public to provide feedback in an inclusive manner that prevents discrimination of groups (e.g. feedback can be provided without needing access to specific devices or system connections).

In particular, personnel from the biometric system owner operating the system shall be able to provide operational experience feedback to the biometric system provider and notify any possible defect.

EXAMPLE A reporting process allows biometric system operators to report if their experience with the system suggests the existence of some demographic differential with the performance of the system.

10.5.4 Threshold management

The threshold value of the comparison score, which indicates a positive match between a capture subject and a candidate in the biometric reference database, has a significant impact on system performance. As described in 8.1, comparison scores returned by a BISPCS should be interpretable by the biometric system owner and this interpretation should be stable throughout the system life cycle. This property makes the management of the operational threshold easier.

EXAMPLE The biometric system owner determines the threshold corresponding to the desired setting for FPIR and FNIR by consulting the test report of the system. The biometric system owner can then continue to use the same threshold throughout the system life cycle unless the desired FPIR changes.

Any change of threshold value shall be recorded.

10.6 Improvement

10.6.1 Retraining of ML-based biometric systems

ML-based biometric system performance can be improved if production data, as defined in ISO/IEC 22989, is used to adapt the system to the conditions observed in real deployment.

When using production data for model training, it shall be checked that the use of this production data is consistent with any licence or user-generated content restrictions.

NOTE Any licence limits on data retention can also apply to models trained on these data, as models are considered a derivation of the training data.

Training the system by using only production data can be challenging as the extent of available production data is not necessarily sufficient nor adequately supervised. In such cases, an alternative strategy is to train the machine learning model with the available data before retraining with additional supervised data coming from an operational system.

EXAMPLE Weights of a trained neural network are used as an initialization for a new machine learning model being retrained with additional production data after supervision.

Normally, the biometric system provider is responsible for the performance of the system, while the production data is under the responsibility of the biometric system owner. The process of development can become more difficult when the biometric system provider and the biometric system owner are two distinct entities.

In order to enforce developer accountability on model performance and to avoid loss of control over system behaviours, model retraining should only be performed by the biometric system provider. Systems should exclude by default the capacity for biometric system owners to retrain models without the support of the biometric system provider. Nevertheless, retraining may be performed by the biometric system owner under the guidance and based on the instructions of the biometric system provider. In some cases, the need for an independent retraining by the biometric system owner is foreseeable and a specific framework is developed and proposed by the biometric system provider.

If a biometric system owner retrains a machine learning model without support from the biometric system provider, the biometric system owner shall be responsible for all aspects of operational performance from that point forward.

If the system is retrained, its performance after the update should be compared with that before the update as described in 10.5.2.

The privacy measures described in 10.4 shall be fulfilled during re-training. Specific measures to allow and protect personally identifiable information shall be specified and implemented to mitigate risk of data leakage outside of the production system. Any need of data sharing from the biometric system owner to the biometric system provider shall be thoroughly justified, with assessment of risks, and such data sharing should be avoided where possible.

10.6.2 Continuous learning

Continuous learning, where production data is used for the incremental update of the system during production, shall not be implemented.

10.6.3 Continual improvement

Biometric systems are under continuous development. Upgrades can become available after the deployment of the system. These updates can be related to hardware, with a change of capture devices or software, or with a change of machine learning model. Any software or hardware upgrade or update shall be properly evaluated.

As a result of the performance evaluation, if a regression relative to the performance measured at deployment is observed, the biometric system owner shall take steps to improve the performance of the

BISPCS with support from the biometric system provider. This can involve diagnostics to identify the reasons for regression, for example, the quality of captured biometric characteristics is low or the demographics of the capture subjects differ from initial specifications. This can take place through adjusting settings of biometric sensors or retraining models with support from the biometric system provider.

System performance can also be improved by optimizing parameters. The impact on performance shall be monitored in accordance with 10.5.2.

Annex A
(informative)

Use case profiles

A.1 Uses cases for law-enforcement investigations using face recognition

A.1.1 General

The World Economic Forum published a white paper on the responsible use of face recognition technology (FRT) for law enforcement.[8] This annex presents the different use cases described involving passive capture subjects.

The different examples presented in the following subclauses follow the practices of the Netherlands Police. These practices can vary across jurisdictions.

A.1.2 How facial recognition is used for law enforcement investigations

Law enforcement investigators use FRT for identification and verification purposes. Identification activity (also referred to as "one to many") consists of searching for the identity of a person, as opposed to verification activity (also referred as "one to one"), which consists of verifying someone's identity against an identity document (ID). Facial examiners are experts who run facial recognition analysis. In the case of the Netherlands Police and INTERPOL, for example, the examiners operate autonomously from the investigation teams, and do not have knowledge of the prosecution that requires them to run facial recognition analysis.

To identify an unknown suspect or person of interest, investigators work with biometric probes and biometric reference databases.

There are two typologies of biometric reference databases:

— Type 1: A biometric reference database of known criminals and suspects, composed of biometric data lawfully collected and stored by law enforcement agencies. People in this biometric reference database are still suspects or have usually been convicted of a crime.

— Type 2: A special biometric reference database built specifically for an investigation. The public prosecutor provides a warrant to seize the video footage of a crime scene. This biometric reference database can be built out of multiple sources (VSS, social media, electronic devices, etc.). All of the faces are detected on the footage and stored on the special biometric reference database. The face of a possible suspect can then be searched against the special biometric reference database to see if the suspect is present on the footage. At the end of the investigation, the biometric reference database is removed from the operational system and stored so that the fact-finding/archiving/evidence file can be produced in court when requested during the judicial procedure.

Biometric probes are images that are part of the law enforcement investigation, and which are submitted to a facial recognition system to be compared to a biometric reference database. Biometric probes are usually the photos or movies/stills of suspects or persons of interest. To collect these images, investigators (or digital/face experts) either already have an image of the suspect or they extract it from footage of movies/stills. Law enforcement tries to collect the best quality image to improve the chance of confirming the identity of the person.

Based on the practices followed by the Netherlands Police, the process for using FRT for law enforcement investigations is as follows:

— Step #1: A (possible) crime is reported or suspected. An investigative team, under the supervision of the public prosecutor, is created and requests warrants to collect images relevant to the crime, including images of the suspect(s). If suspects are detected on the images, the team will try to determine their

identity. This can be done by human means (through recognition by people who know the suspects, e.g. police officers or witnesses) or by using facial recognition software with a biometric reference database of known people (e.g. suspects and convicts).

— Step #2: If a facial recognition search is required, the investigation team will apply for an FRT investigation through the specialized FRT team. This facial examination team runs FRT software to compare the biometric probe against one or multiple biometric reference databases. Before doing so, the facial examiners will first judge the quality of the biometric probe. If suitable for an FRT search, they will enter the biometric probe into the FRT system, allow the system to do the pre-search analysis and may also provide some notable facial landmarks (centre of the eye socket, etc.) to the software. The examiners then set up the FRT software at a setting that is not too narrow, to avoid false negatives, or too wide, to avoid false positives, which would result in a list of candidates too large to be of use.

— Step #3: After the search, the facial examiners analyse the list of candidates provided by the software. They run this last operation manually, deploying their expertise to check if one of the candidate images proposed by the system matches the biometric probe.

— Step #4: If the facial examiners make a possible match, only the biometric probe image and the image of the possible candidate from the biometric reference database are handed to two facial experts. They perform, independently from each other, a full analysis of the biometric probe and the reference image to determine the similarity/dissimilarity between the two faces. This blind peer manual review is systematically performed before any positive result is communicated to the requesting investigation team. The facial examiners and experts do not know the exact background to the case, to avoid bias as far as possible. The end result is the final consensus conclusion and is reported to the investigation team as an investigative lead.

A.1.3 Example scenarios

A.1.3.1 Finding the identity of an ATM fraud criminal

Fraudulently obtaining bank account data by usurping someone's identity allows a person to access a bank account and withdraw cash from an ATM machine. The video footage from the ATM machine enables investigators to collect a facial image of the offender. The quality of this image will vary depending on the exposure and whether the fraudster managed to hide their face. If the quality of the image is good enough, the photo collected will be compared against a biometric reference database of known criminals using a facial recognition system looking for a matching candidate. If facial examiners confirm a possible match, they follow the standard process described in Step #4 presented in A.1.2.

A.1.3.2 Uncovering the identity of a person assaulting a police officer

A person attacks police officers and footage of the incident is collected from VSS cameras. An investigation is launched and a warrant is provided to an investigation team to seize these images. The goal is to identify the assailant. To that end, the investigators, with the help of the police's digital experts, manually review the VSS/video footage of the incident, looking for images of the wanted person. They collect images with the best possible angle, lighting and exposure to increase the quality of the image(s) and give the best chance of obtaining matches and identifying the person. If facial examiners make a possible match, they follow the standard process described in Step #4 presented in A.1.2.

A.1.3.3 Looking for the identity of a museum thief

A piece of art has been stolen in a museum. A public prosecutor launches a criminal investigation. The investigation uncovers the identity of a potential thief and a warrant is given to collect video footage from the museum. Then, using a facial recognition tool, the investigators collect images of the faces of all visitors and staff who appear in the footage and build an investigation biometric reference database from it. A list of candidate images is displayed by the system, manually reviewed and analysed to establish whether a serious potential match is detected that would confirm the involvement of the suspect. If facial examiners make a possible match, they follow the standard process described in Step #4 presented in A.1.2.