INTERNATIONAL STANDARD

ISO/IEC 24714

First edition
2023-07

Biometrics — Cross-jurisdictional and societal aspects of biometrics — General guidance

Biométrie — Aspects transjuridictionnels et sociétaux de la biométrie — Partie 1: Recommandations générales

Reference number
ISO/IEC 24714:2023(E)

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*.

This first edition of ISO/IEC 24714 cancels and replaces ISO/IEC TR 24714-1:2008, which has been technically revised.

The main changes are as follows:

— addition of privacy by design and privacy by default principles;

— addition of examples.

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

This document provides support for the further development of ISO/IEC biometric International Standards in the context of cross-jurisdictional and societal applications of biometrics, including standardization of both existing and future technologies.

Specifically, this document offers guidance on the design of systems that use biometric technologies to capture, process and record biometric information:

— with regard to societal norms and legal requirements of jurisdictional domains (within and among various levels of jurisdictions);

— pertaining to privacy/data protection of an identifiable individual;

— with respect to an individual's ability to access and use these systems and the information they contain;

— with regard to health and safety issues pertaining to an individual when systems are utilized to capture biometric data.

In this document, biometric data are considered to be personally identifiable information (PII).

Examples of the benefits to be gained by following the recommendations and guidelines in this document are:

— enhanced acceptance of systems using biometrics by subjects;

— improved public perception and understanding of well-designed systems;

— smoother introduction and operation of these systems;

— potential long-term cost reduction (whole life costs);

— increased awareness of the range of accessibility-related issues;

— adoption of commonly approved good privacy practice.

The primary stakeholders are identified as:

— operators – those who use the results of the biometric data,;

— developers of technical standards;

— subjects – those who provide a sample of their biometric data;

— writers of system specifications, system architects and IT designers;

— public policy makers.

Biometrics — Cross-jurisdictional and societal aspects of biometrics — General guidance

1 Scope

This document gives general guidance for the stages in the life cycle of a system's biometric and associated elements. This covers the following:

— the capture and design of initial requirements, including legal frameworks;

— development and deployment;

— operations, including enrolment and subsequent usage;

— interrelationships with other systems;

— related data storage and security of data;

— data updates and maintenance;

— training and awareness;

— system evaluation and audit;

— controlled system expiration.

The areas addressed are limited to the design and implementation of biometric technologies with respect to the following:

— legal and societal constraints on the use of biometric data;

— accessibility for the widest population;

— health and safety, addressing the concerns of users regarding direct potential hazards as well as the possibility of the misuse of inferred data from biometric information.

This document is intended for planners, implementers and system operators of biometric applications.

Specification and assessment of government policy are not within the scope of this document. However, this document is intended to be beneficial to public authorities when deploying biometric systems.

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given 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
accessibility
extent to which products, systems, services, environments and facilities can be used by people from a population with the widest range of user needs, characteristics and capabilities to achieve identified goals in identified contexts of use

Note 1 to entry: Context of use includes direct use or use supported by assistive technologies.

[SOURCE: ISO 9241-112:2017, 3.15[1]]

3.2
data subject
subject
individual whose individualized biometric data is within the biometric system

Note 1 to entry: The data subject is the data principal of PII.

[SOURCE: ISO/IEC 2382-37:2022, 37.07.05, modified — The original term "biometric data subject" has been changed to "data subject" and Note 1 to entry has been replaced.]

3.3
function creep
expansion of a project, mission, or system's function beyond its original goals

Note 1 to entry: Function creep is the result of the intended or unintended change or extension to the functions of a system, which occur as small incremental stages, and can lead to significant changes to the function.

3.4
proportionality
balance between the interests of an individual and the interests of an organisation

3.5
usability
extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

Note 1 to entry: The "specified" users, goals and context of use refer to the particular combination of users, goals and context of use for which usability is being considered.

Note 2 to entry: The word "usability" is also used as a qualifier to refer to the design knowledge, competencies, activities and design attributes that contribute to usability, such as usability expertise, usability professional, usability engineering, usability method, usability evaluation, usability heuristic.

[SOURCE: ISO 9241-11:2018, 3.1.1[2]]

3.6
personally identifiable information
PII
any information that a) can be used to identify the PII principal to whom such information relates, or b) is or might be directly or indirectly linked to a PII principal

Note 1 to entry: To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

Note 2 to entry: In this document the PII principal is the data subject.

[SOURCE: ISO/IEC 29100:2011, 2.9[3].]

4 Symbols and abbreviated terms

API	application programming interface
DPIA	data protection impact assessment
DPO	data protection officer
FRR	false reject rate
FAR	false accept rate
GDPR	general data protection regulation
HTTP	hypertext transfer protocol
ICT	information and communication technology
IT	information technology
PET	privacy enhancing technology
PIN	personal identification number
REST	representational state transfer NOTE REST is an architectural style that defines a set of constraints and properties based on HTTP.
UCD	user-centred design
UI	user interface

5 Cross-jurisdictional and societal considerations

5.1 General

This document provides generic recommendations that are not specific to technologies or applications and that can affect all biometrics.

This clause begins by providing principles, guidelines and considerations for the design and implementation of biometric applications in three major areas:

1) cross-jurisdictional issues related to privacy and protection of personal information (see 5.2);

2) accessibility (see 5.3); and

3) an examination of health and safety issues when using biometric applications that can affect design and implementation considerations (see 5.4).

It considers usability and highlights conditions of the physical environment that can affect the operation and usability of a biometric application (see 5.5), societal, cultural and ethical aspects of biometrics (see 5.6) and acceptance of the use of biometric applications (see 5.7).

Two use cases are provided in Annex A as practical illustrations.

5.2 Cross-jurisdictional issues

5.2.1 General

The developer of a biometric application should take into account a number of issues that relate to specific jurisdictional requirements, which can differ between jurisdictions, not all of which are within the scope of this document. The list of issues which have not been examined in detail in this document includes:

— anti-discriminatory laws;

— disclosure laws;

— redress mechanisms;

— contractual issues;

— provision of biometric data to parties other than the data holder;

— provisions for law enforcement agencies for access to biometric and associated information;

— opt-in and opt-out rights and associated requirements for fall-back processes;

— specific data retention conditions (including period of time and security standards);

— evidentiary requirements for use of biometric data in a court of law;

— specific instances where biometrics are required by organizations or governments (e.g. for secure access to military facilities and critical infrastructure);

— applicability of legal domains in use of biometrics on the internet;

— border control laws.

5.2.2 Privacy aspects of biometric applications

With the proliferation of biometric applications worldwide, the aspect of privacy gains importance. As a result, it is necessary to understand what the objectives of data protection law and policy intend. It is necessary that the applicable law and policy protect data subjects and their biometric data and personal rights. Using a biometric application means using PII; thus, existing privacy laws apply. Depending on how a system is deployed, biometric technology can compromise or protect a data subject's privacy. The possibility of protection is especially valid in view of the special properties of biometrics, which are linked uniquely to the subject for their lifetime, unlike PINs and passwords, which are indirectly and weakly linked to a person. By using a biometric key, other types of PII can be better protected from theft and misuse than by traditional means. Biometrics can therefore be both an object and a tool in the different aspects of this discussion. In all applications, the principle of proportionality should be applied. That means that biometric data used should be adequate, relevant and non-excessive with regard to the purposes for which they are collected and further processed.

Biometrics can be considered in the context of PETs. PETs are a coherent system of ICT measures that protect privacy by eliminating or reducing PII or by preventing unauthorised, unnecessary and/or undesired processing of PII; all without losing the functionality of the data system.

NOTE 1 Processing in this context includes any operation or set of operations which is performed upon PII, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

The principle of PET applies to biometrics seen from two standpoints:

— as an object of the principle, the implementation and application of biometrics should follow a comprehensive and correct privacy regime in order to be privacy enhancing;

— as a tool in the meaning of PET, biometrics itself can be a privacy enhancing method.

For instance, biometrics can improve the verification process compared with a traditional process where a subject has to provide information through requested evidentiary documents which can reveal considerable personal information. The use of biometrics can simply be putting a fingerprint on a sensor without revealing any additional personal information (name, address, date of birth, etc.) to the person who is checking the entitlement of the identified person (given that there has been a proper registration process beforehand). Moreover, the use of biometrics enables the subject to bind a device (such as a smart phone) to their identity. The advantage is that, although a device can have more than one user, the biometrics bind the use to a single specific identity. Subjects can use pseudo-identities by varying the biometrics provided.

The following are some generally accepted rules of PETs.

— At the planning stage, assess whether or not biometrics should be used or another less intrusive method substituted

— Use no PII or as little as necessary.

— Use encryption if using PII.

— Destroy raw data as soon as possible.

— Anonymize PII wherever possible.

— Do not use central databases where not required.

— Give subjects control over their PII.

— Use a means of evaluation and certification to verify that an application delivers a guarantee of an appropriate level of trust.

NOTE 2 See also ISO/IEC 24745[4].

In relation to privacy, Article 17 of the International Covenant on Civil and Political Rights[14] stresses that no one's privacy, family, home or correspondence should be subjected to arbitrary or unlawful interference, nor should their honour and reputation be unlawfully attacked.

Privacy is one of the most significant issues confronting not only the biometrics industry, but also any organization which gathers personal information. The potential for shared access to information and multiple uses of biometric databases raises specific concerns. However, many statements on privacy fail to capture the nuances across various biometric deployments. Certain types of biometrics engender a greater perception of privacy invasion while others have little influence on privacy concerns. PII is the first step to establishing personal identity and it is at this point where many crimes of identity occur. Although there are many issues associated with submitting biometric data, it should be reinforced that identification will have already been established through other identity documents such as birth certificates. Therefore, many people might consider biometric techniques to be far less invasive than being asked, sometimes face to face, questions relating to their personal history, details of residence and information about other members of their family, such as a mother's maiden name. In this context, biometric technology is simply another means for identification.

The increasing number of implementations and discussions about the use of biometrics raises questions about the technology's impact on privacy in applications generally available and widely used by the public, in the workplace and at home. Key aspects of privacy issues relate to either the data subject or the organization. From the data subject's perspective, issues relate to collection, choice, use and security of information and anonymity of the individual. From an organizational perspective, issues include the manner and purpose of collection, solicitation, storage and security of information, access to records, relevance and the limits on use and disclosure of collected data.

Other privacy issues relate to concerns that include stigmatization and reputational or financial damage. An example of stigmatization in some communities has been the association of fingerprints with criminal activity. However, fingerprinting is now also becoming associated with the more positive

identification of the law-abiding citizen as a holder of electronic ID documents, a cardholder, or club member. Any concerns can be exacerbated by the possibility that a person's biometric can be "spoofed".

Further privacy issues relate to function creep, or the misuse of information, and tracking or aggregation of data. In relation to function creep, using data for a secondary purpose can appear worthwhile; however, socio-cultural and legal issues can arise when individuals are not informed of this secondary purpose for which their information will be used, and have not given consent for this to take place. "Tracking" can refer to a specific form of function creep where biometric data is used in combination with additional data such as spending or travel details to track the actions of individuals. Covert use of biometrics without legal authorization will impinge on individuals' privacy.

In addition to the analysis of cross-jurisdictional issues relating to privacy listed in 5.2.3, a number of other considerations should be taken account of, including:

— issues relating to the linking of biometric data to other information;

— transition states, e.g. the ability to give consent changes:

  — migration from a minority to a majority age,

  — change in mental capacity (e.g. Alzheimer's disease),

  — death of a subject,

  — revocation procedures;

— notification to anonymously enrolled data subjects of any changes in the uses of a biometric.

The system data protection officer, or equivalent, should take part in the planning and implementation of all biometric applications. They should also drive the development and implementation of the biometric privacy policy and ensure conformance to that policy. Where there is no data protection officer, there should be a person in charge of implementing the system who is able to deal with IT security and privacy issues when they occur.

If recognized national consumer associations have published recommendations on biometrics that seem to be applicable to a specific biometric implementation, a system operator should consider them where appropriate.

5.2.3 Privacy principles for biometric applications

There are a number of key privacy-enhancing principles that should be considered by organizations implementing a biometric application. These principles, which are listed below, build upon the reference documents listed in the Bibliography. They should be considered and applied in the context of jurisdictional laws and regulations.

1) Transparency

   There should be a general policy of openness about the use of biometric data, which should include the purposes for which the data is to be used and the point of contact responsible for its use. Any subsequent changes should be made known to data subjects.

2) Consent

   Biometric data should be collected, stored, used, disclosed and retained with the knowledge and consent of data subject, except where local laws have exemptions to this principle.

3) Preference for opt-in

   Where feasible and practical, opt-out or opt-in procedures should be made available to the data subject. In general, opt-in is the preferred option.