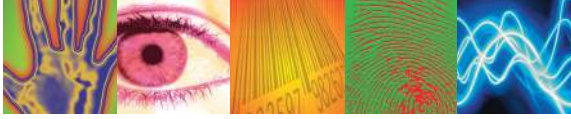
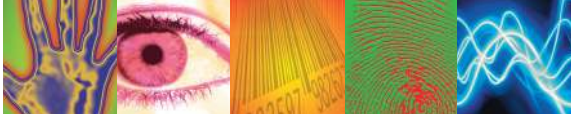


BIOMETRICS™ INSTITUTE

Biometrics Privacy Guidelines

A Best Practice Guide for Biometrics and Privacy

www.biometricsinstitute.org



BIOMETRICS™ INSTITUTE

Biometrics Privacy Guidelines

Purpose of the Biometrics Privacy Guidelines

The Biometrics Privacy Guidelines are designed by the Biometrics Institute to:

a) Guide vendors and suppliers, individuals/data subjects, researchers, operators, managers/controllers and purchasers of biometric systems.

b) Assure the public that the managers/controllers have followed best practice privacy principles when designing, implementing and managing biometric based projects.

c) Be a guide across many different countries and jurisdictions, recognising that biometrics and information technologies do connect beyond national boundaries and across different fields as diverse as health records, border controls, identity documentation, retail, consumer based applications in the telecommunications industry, finance and banking and drivers' licenses.

Note that you will need to be compliant with the legislation that prevails in the countries and jurisdictions where you operate, noting that some jurisdictions have specific legislation and rules relating to specific areas such as personal health records. However, not all legislation can cover changes in technology and business strategies in a timely manner. The Guidelines, being a best practice guide, are specifically designed to fill that gap.

Since the Guidelines will operate across different countries, sectors and levels of expertise, your attention is drawn to the Definitions Section where an attempt has been made to standardise terms and describe them in layperson's language.

We strongly recommend that managers/controllers (sometimes called Data Protection Officers) dealing with biometrics on an international level familiarize themselves with the new European Union General Data Protection Regulation (EU GDPR) which extends both its territorial and compliance coverage (See http://www.eugdpr.org/). Managers/controllers must ensure that privacy is designed into all biometrics projects at the earliest planning stage.

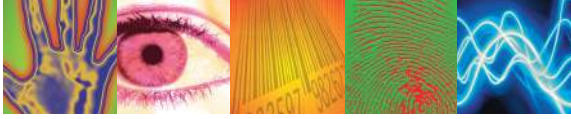
Definition of Biometrics

These Guidelines are jurisdictional and technology neutral and accept the following definition of biometrics of the International Organization for Standardization (ISO); "automated recognition of individuals based on their biological and behavioural characteristics."[1]

About the Biometrics Institute

The Biometrics Institute was established in Australia in 2001 and is now operating at an international level with an office in London and Sydney. It runs regular meetings for its members in Australia, Europe, New Zealand and the USA. Its members cover a wide range of users (such as banks and airlines), government agencies, law enforcement authorities, academia and vendors. The Biometrics Institute's constitution requires that users are represented on the Board so independence is assured by the majority control being vested in users. This guarantees independence from commercial control but assists vendors to act as good corporate citizens

1 *ISO/IEC 2382-37: Information technology — Vocabulary —Part 37: Biometrics, December 2012*



BIOMETRICS™ INSTITUTE

Biometrics Privacy Guidelines

The Key Principles of the Guidelines

Principle 1 Respect for Individuals/Data Subject Privacy

The first principle of these Guidelines is respect for individuals/data subject privacy. All other principles are guided by respect for the fact that the individuals/data subjects, in providing a unique physical attribute of themselves to another party, are entitled to expect that the recipients and processors understand and discharge their responsibilities as guardians of that biometric and associated personal data.

Within an organisation using biometrics, all staff and management should commit to protection of privacy, demonstrate a respect for individuals/data subject privacy and implement plans to control the use of biometric data and other personal data in a systemic manner. This would include the critical activities outlined in Principles Fourteen and Fifteen.

Managers/controllers must ensure that privacy is designed into all biometrics projects at the earliest planning stage.

Principle 2 Proportionality

When considering the business case for the use of biometrics, consider if such a technology choice could constitute a privacy risk and if that risk is proportional to the business benefits.

Principle 3 Informed Consent

A person's right to give informed consent should be respected where possible. This includes the right to know;

a) why and when the biometric is collected,

b) who is collecting it,

c) who else will have access to it,

d) how it will be protected, stored, transmitted and accessed,

e) the time limits on its use and storage

f) how a person can know if modifications are made to the above or if any part is sold on

g) how inaccurate/ bad quality information and biometrics can be updated or corrected

h) access rules for other authorities such as law enforcement agencies and private organisations working alone or in partnership with public authorities

i) rules that protect minors where parents are not readily available to make an informed decision

j) rules that require how individuals/data subjects will be informed about key issues such as privacy breaches, the remediation of those breaches and the liabilities that the system owners have.

k) how individuals/data subjects can opt out or have their biometric deleted.

Wherever possible, systems should be designed so that individuals/data subjects can opt-in to the system rather than being automatically included. If, for reasons such as law enforcement or some medical issues, opt-in is inappropriate, the reasons should be documented for audit and review purposes and made available in writing to the individual/data subject unless there are legal or professional reasons not to do so.

All managers/controllers should factor into their planning the EU GDPR relating to lawful processing including informed consent and withdrawal, consent of minors and the subject's withdrawal of consent.
(Articles 6, 7 and 8).

All information relating to the above should be expressed in plain language with key information being presented first and not hidden at the end of such information

Principle 4 Truth and Accuracy in Business Operations

Vendors or suppliers and managers/controllers should provide accurate and honest information about the biometric system, especially its efficacy, reliability and its effects on privacy protection, and potential linkage to other information that may identify or be associated with individuals/data subjects.

Vendors or suppliers, managers/controllers and operators should also provide accurate and honest information about their capacity to update their systems to counter emerging new risks and threats

Principle 5 Protection of Biometric Data Collected

The manager/controller should be accountable for protecting biometric data collected. This should include Privacy Impact Assessments (PIA) (a copy of the Biometrics Institute's model PIA will be available from the second half of 2017), Privacy Audits, clear privacy policy procedures and policies and technical controls over such issues as unauthorised access, accidental loss or misuse of personal data. Wherever possible or feasible, it is desirable to separate the biometric template/samples from the data subject's other identifying information.

Procedures for reporting privacy breaches plus remediation policies and applicable penalties in the event of a breach should be made available to all staff and to individuals/data subjects. This also applies to vendors that licence biometric technologies to other organisations; such vendors should also provide the above procedures.

Principle 6 Complaints and Enquiries

Managers/controllers of biometric systems should have in place complaints and enquiry systems which include transparent avenues for redress and a sympathetic approach which accepts the possibility of procedural or technical faults in their biometrics system.

This above applies particularly to identity theft or situations where individuals/data subject information has been either lost or stolen, compromised or inaccurately recorded. Managers/controllers must have in place convenient but robust processes to repair or re-instate that damaged personal data. This may include a compensation process.

Principle 7 Purpose

The managers/controllers should, wherever possible, clearly identify the purpose of the collection or use of biometric data and should not use that data for purposes other than that stated purpose.

Principle 8 Non Discrimination

Managers/controllers should aim to ensure that no person will be denied service or access due to their inability to provide a biometric or use a biometric system. An alternative should be offered where possible and system design should include alternative processes for those unable to access that system, including provision of access at a later date.

This should include identifying any options for exempting persons who cannot use the system for reasons of disability, inability to enrol, conscientious objection or cultural or religious beliefs.

If system managers/controllers cannot provide the above exemptions, the reasons should be documented for audit and accountability purposes.

Principle 9 Accountability

Each organisation that deals with biometrics should have a trained and trusted officer or designated external consultant who is accountable for the design and management of privacy protection.

Where contractors and other providers are used by managers/controllers to design, build or operate biometric systems, the principal must ensure that privacy protections and accountability are designed into the systems and that contractual obligations to protect privacy are in place and are monitored and audited regularly.

Principle 10 Sharing of Biometric Data

All individuals/data subjects should be informed of circumstances where data may be shared with other parties whether for law enforcement purposes or fraud investigations or other purposes relating to law and order or commerce. This may be done through a general warning but individuals/data subjects should be made aware of that possibility.

Principle 11 Provision of Advance Warnings of Surveillance

Where biometrics are abstracted from or used for surveillance purposes such as in CCTV monitoring, there should be forward warnings that such surveillance may take place, except where law enforcement or border control purposes require secrecy.

Principle 12 Transmission of Biometric Data Beyond National Boundaries

This should only be done wherever the data protection regime in that other jurisdiction is greater than or equal to that which prevails in individuals'/data subjects' own country or jurisdiction and should involve prior warning (even if generic) that such a transfer can take place. Wherever possible, systems should be designed so that they are not reliant upon the need to transfer such data between countries, except for clearly stated law enforcement or border control purposes. Even if technologies and business cases require cross jurisdictional transfers, the collectors of that personal data should understand that they have an ongoing responsibility for what happens to the data, including its linkage to other data such as that associated with financial transactions and ecommerce.

Managers/controllers are again reminded that the EU GDPR should be factored into planning given that those regulations will affect any organisation that collects or uses the data of European Union citizens, regardless of whether or not that organisation is based in the European Union.

Principle 13 Employee Biometric Data Must be Protected

Wherever employees are required to provide biometric data to their employers, that data should be protected in accordance with the provisions of Principles Five and Nine. Where an employee's biometric data is collected as part of surveillance, the possibility of that surveillance should be made known beforehand to the employee. Upon cessation of employment, the former employee's biometric data should be destroyed within a reasonable period after that cessation unless there are justifiable reasons not to do so.

Principle 14 Limit the Extent of Personal Data Exchanged and Retained

Wherever feasible, biometric system design should be based on the principle of minimising transmission of personal data among sub-components of the system. A yes/no or green light/red light permission regime should be the first principle of transactions within the system. Personal Data should not be retained once its purpose and use has expired, unless there is end user consent or a legal requirement to retain that data (such as in archive legislation)

Managers/controllers and system designers should examine the usefulness of technologies and systems where the biometric is controlled primarily by individuals/data subjects.

The attention of managers/controllers is drawn to the EU GDPR regarding erasure of personal data sometimes known as "the right to be forgotten" (Article 17).

Principle 15 Maintain a Strong Privacy Environment

Any business plan involving the use of personal data such as biometrics should begin with a PIA to identify privacy risks and document methods planned to protect privacy. A Biometrics Institute model PIA will be available from the second half of 2017.

In order to ensure privacy accountability within a system, it is essential to maintain time dated privacy logs which should encompass technical controls, records of privacy breaches or incidents, documented procedures for notification of privacy breaches and a regular review of those logs to ensure that the privacy environment does not deteriorate.

Privacy Audits should be conducted by independent experts at regular intervals in order to assess the whole organisation's management of privacy.

Procedures should be in place to repair or re-instate personal data that has been stolen or damaged in any way. Individuals/data subjects who have experienced identity theft should have their problems resolved in a speedy and sympathetic manner.

Principle 16 Maintain Privacy Logs

This principle is based on OECD Privacy Principle 7 (http://oecdprivacy.org/) and the EU GDPR. It concerns the right of a data subject to have access to their own data and to correct it if it is in error or degraded. In the case of biometric data this would be the right to ensure that a biometric sample has been associated with the correct data subject.

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him/her;

b) to have communicated to him, data relating to him within a reasonable time at a charge, if any, that is not excessive in a form that that is readily intelligible to him/her;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him/her and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Further, biometric systems should be designed to allow data portability so that the individual/data subject can receive their personal data in commonly used but secure format for transmission to another controller in another organisation. Managers/controllers are reminded that EU GDPR may oblige them to do this (Article 20).

Recommendations for Implementing and Managing the Principles of these Privacy Guidelines

a) Examine the business case for using a biometric. Determine whether or not biometrics are really required or are there other technologies or procedural alternatives. Look at the business and stakeholder needs and perceptions. Check to see whether the business case can include Principle Eight which should include where possible, an alternative for those end-users unable to participate.

b) Select the biometric to match the business case; examine the costs and efficacy and look for privacy enhancing designs and technology.

c) Identify on record for later reference, relevant government privacy acts, directives, regulations or other privacy codes with which your organisation should or must comply. To avoid later re-engineering of the selected biometrics system it is good planning to ensure that your selected system will be compliant across all relevant jurisdictions (such as European Union companies which may seek at a later date to enter the US market, and vice versa.)

d) Conduct a PIA to determine the privacy issues, level of risk and solutions, legislative or policy constraints. For example, does the selected biometric system enable managers/controllers or commercial partners to later gather or sell extracted data in a way that the original biometric donors would consider privacy invasive? Are the designers and vendors and suppliers of the biometric system examining options to protect the biometric template and associated personal identifiers from hacking or being compromised? Is separation of template and those personal identifiers appropriate or will that separation prevent restoration of hacked templates and associated identifiers?

e) In order to maximise individuals'/data subjects' co-operation and acceptance, plan to test the proposed system with them at an early stage. Include user friendliness and privacy in that testing. This should include testing of the language and style used to inform individuals/data subjects about their privacy rights.

f) Ensure sign off and commitment for the project from senior officers; determine accountability and responsibilities.

g) Build a communications strategy to ensure that there is stakeholder commitment and understanding and that media, parliamentary and public perceptions are recognized and dealt with; the strategy should also include a privacy awareness campaign for the company or agency using the system.

h) If using contractors, ensure that they are governed by contractual and procedural controls about privacy. This should include the right of the manager/controller to conduct audits and demand explanations from the contractors. You cannot entirely outsource risk, especially if you are a public agency accountable to legislatures.

i) Test the system design and pilot off-site before migrating it to the production environment. Include in this testing an assessment of the biometric accuracy and vulnerability of the system to attacks that could compromise privacy.

j) Recheck the design and implementation plans against your original compliance record suggested in section 5 (c) of these Guidelines.

k) Monitor the achievement of those milestones that have been set during the selection of the design and implementation team.

l) Ensure that privacy logs are kept up to date and are available for independent auditors and those conducting PIAs.

m) Put in place annual or regular Privacy Audits that examine and report on privacy compliance and can detect any degradation of the privacy environment. Senior management and those responsible for privacy management should be regularly briefed in writing about risks and identified issues and this should be available to the independent auditors. The auditing personnel should report to a high-level officer in the company or agency.

n) Design in the policies and procedures for any possible decommissioning given that even a decommissioned or failed data collection project may contain live and/or sensitive personal data.

o) Join an independent biometrics group such as the Biometrics Institute in order to help build your organisation's biometrics and privacy awareness and keep in touch with best practice and technology advances.

Definitions

In this section, the Biometrics Institute has provided definitions that, as far as possible, have similar meanings around the world. Some jurisdictions may find some of the definitions unfamiliar but the benefits of attempting some uniformity are obvious.

Another useful reference guide for terminology is the ISO/IEC 2382-37: Information technology — Vocabulary — Part 37: Biometrics, December 2012.

Biometrics, Biometric systems	Means the automated recognition of individuals based on their biological and behavioural characteristics.
CCTV	Closed Circuit Television
Client/Owner/Manager/Controller	A person or entity owning, buying or commissioning a biometric system or service; a client is also sometimes used to describe an individual end user but that meaning is not used in these Guidelines.
Contractor	An entity or person who is engaged to conduct services or work on behalf of a major client.
Customer	A person or entity buying and using a biometric system.
Individual/Data subject	A person providing and using their own biometrics; sometimes called a client or end user when referring to an individual, sometimes called a biometric donor.
Managers/Controllers	Those who manage the planning, implementation and ongoing decisions about a biometric system. A Data Protection Officer is used often to describe a person who is responsible for data protection compliance.
Minor	A person under the legislated age of being able to exercise independent adult responsibility.

Decommission	To take out, in this scenario, a biometric system.
Privacy Audit	An analysis by an independent third party of a project or entity's privacy environment, covering such issues as technical and procedural privacy protection, privacy awareness programmes, threats and risks, incident reporting.
Privacy Impact Assessment (PIA)	A pre-implementation assessment of the impact on privacy of a planned change in business activity (See ISO/IEC 29134 for further definition)
Privacy Logs	Auditable logs of those who have had access to personal biometric data bases and the reasons for that access; also should contain records of privacy breaches or incidents and the action taken to investigate and report. They should include any conclusions reached plus any systemic improvements that arise from those investigations.
Production Environment	Live use of an IT based system as opposed to a test or pilot site.
Biometric Data Subject	Individual whose individualised biometric data is within the biometric system[2]. Data subject means an individual who is the subject of personal data[3].
Vendor or Supplier	A seller of services or product.

Further Reading

There are certain standards with which organisations should be familiar. In particular, your attention is drawn to:
OECD Privacy Principles http://oecdprivacy.org/
European Union General Data Protection Regulations (EU GDPR) fully operational across all EU countries by May 2018. http://www.eugdpr.org/
The ISO standards related to biometrics at the following link
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=on.
ISO/IEC 24745:2011, Information technology – Security techniques – Biometric information protection
ISO 27002, Payment Card Industry (PCI) Data Security Standards (DSS) and the Federal Financial Institutions Examination Council (FFIEC)'s IT Examination Handbook
ISO 29100: 2011, Information technology – Security techniques – Privacy Framework
ISO/IEC 2382-37: Information technology — Vocabulary —Part 37: Biometrics, December 2012
ISO/IEC 29134: Privacy Impact Assessment April 2017
British Standards Institution PAS92:2011 – Code of Practice for the Implementation of a Biometric System.
Privacy Impact Assessments: the CNIL publishes its PIA manual, France, July 2015
https://www.cnil.fr/fr/node/15798
Biometrics Institute Model Privacy Impact Assessment 2017 (to be released in the second half of 2017)
The Biometrics Institute can provide further information as documented Standards or Legislation or Directives changes.

Contact

The Biometrics Institute at:
Email: manager@biometricsinstitute.org
Australasia: +61 2 9431 8688
Europe: +44 7887 414 887
Web: www.biometricsinstitute.org