

CHAPTER 11 – PERSONAL IDENTIFIERS

OVERVIEW

PERSONAL IDENTIFIERS UNDER THE ACT

Section 10 - Personal identifiers

Section 3 - Definitions

OBTAINING PERSONAL IDENTIFIERS– Subdivision A

Section 40 - Request for personal identifiers

Section 41 - Provision of personal identifiers

OBLIGATIONS RELATING TO PERSONAL IDENTIFIERS – Subdivision B

Section 42 - Accessing identifying information

Section 43 - Disclosing identifying information

Section 44 - Unauthorised modification or impairment of identifying information

Section 45 - Destroying identifying information

OVERVIEW

The purpose of this chapter is to provide guidance to DIAC officers on the requirement for, and collection, use, storage and destruction of, personal identifiers for the purposes of the *Australian Citizenship Act 2007* (the Act).

Personal identifiers can only be collected and used to identify, or authenticate the identity of, a person seeking to sit a test (before making an application for citizenship by conferral under the general eligibility provisions), making an application for citizenship or evidence of citizenship, or to assist in combating document and identity fraud in citizenship matters.

If a person is required to sit a test before making an application for citizenship by conferral under the general eligibility provisions the Minister must be satisfied of the person's identity. If the Minister or delegate is not satisfied of a person's identity they cannot sit a test. This is set out in the Minister's determination made under Section 23A of the Act.

Subsections 17(3), 19D(4), 24(3), 30(3), 33(4) and 37(4) of the Act require that, before an application is approved, the Minister must be satisfied of the person's identity. If a person's identity cannot be verified the application cannot be approved.

Division 5 of Part 2 of the Act provides the legislative framework for collecting personal identifiers from people seeking to sit a test, or applying for Australian citizenship or evidence of Australian citizenship.

It is important to recognise that personal information is not the same as personal identifiers.

Personal information is non-specific data such as gender, date and country of birth, occupation and marital status. The use, storage and disclosure of personal information collected for citizenship purposes are all protected under the *Privacy Act 1988*. In contrast, **personal identifiers** are any of the following: fingerprints or handprints of a person (including those taken using paper and ink or digital live scanning technologies); a measurement of a person's height and weight; a photograph or other image of a person's face and shoulders; an iris scan; a person's signature; and any other identifier

prescribed by the regulations, other than an identifier the obtaining of which would involve the carrying out of an intimate forensic procedure as defined in s23WA of the *Crimes Act 1914*. For the purposes of the Act, **identifying information** is any personal identifier which is collected from the applicant for the purposes of the Act, and any additional information which can be used for identification purposes and is obtained either directly or indirectly from a personal identifier collected from a person.

Personal Identifiers under the Act

Personal identifiers Section 10

- “(1) For the purposes of this Act, a **personal identifier** is any of the following (including any of the following in digital form):
- (a) fingerprints or handprints of a person (including those taken using paper and ink or digital liveness scanning technologies);
 - (b) a measurement of a person’s height and weight;
 - (c) a photograph or other image of a person’s face and shoulders;
 - (d) an iris scan;
 - (e) a person’s signature;
 - (f) any other identifier prescribed by the regulations (except an identifier the obtaining of which would involve the carrying out of an intimate forensic procedure within the meaning of section 23WA of the Crimes Act 1914).
- (2) Before the Governor-General makes regulations for the purposes of paragraph (1)(f) prescribing an identifier, the Minister must be satisfied that:
- (a) obtaining the identifier would not involve the carrying out of an intimate forensic procedure within the meaning of section 23WA of the Crimes Act 1914; and
 - (b) the identifier is an image of, or a measurement or recording of, an external part of the body; and
 - (c) obtaining the identifier is necessary for either or both of the following purposes:
 - (i) assisting in the identification of, and to authenticate the identity of, a person making an application under Part 2 or seeking to sit a test approved in a determination under section 23A;
 - (ii) combating document and identity fraud in citizenship matters;”

As defined in section 10 of the Act, a personal identifier is any of the following in actual or digital form:

Fingerprints or handprints of a person

Prints are not currently required to be provided. Prints could be captured anywhere an ink or paper imprint is used or a digital scan of the fingerprint or handprint is taken.

A measurement of a person's height and weight

These measurements are not currently required to be provided. The measurement of a person's height or weight can be taken in any form that provides a meaningful indication of the person's actual individual measurements in order to be best able to appropriately identify the person.

A photograph or other image of a person's face and shoulders

This personal identifier is required to be provided where a person seeks to sit a test (before making an application for citizenship by conferral under the general eligibility provisions) and with an application for citizenship or evidence of citizenship.

When making an application for citizenship, the photograph must be endorsed on the back by a person who meets the policy requirements for the purposes of making a proof of identity declaration. Forms 1195 and 1295 (online applications) have details on the "proof of identity declaration". Policy is that the photograph or other image is to be similar to a passport photo, that is, to be clear and show a person's features enough to allow a person to be recognised by the image.

"Photograph" includes a digital image taken by an officer of the Department.

An iris scan

Iris scans are not currently required to be provided. They would need to be taken by an appropriate biometrics operator and on recognised biometrics software which will enable a positive identification of that person.

A person's signature

This personal identifier is currently required to be supplied with an application where it is a part of the declaration made in respect of that application.

People seeking to sit a test (before making an application for citizenship by conferral under the general eligibility provisions) will also be required to supply

their signature at the time of registration for a test.

Any other identifier prescribed by the regulations

Currently, no additional identifiers are prescribed. The Act limits the types of personal identifiers that can be prescribed. *Intimate forensic procedures* or images of the internal parts of the body can not be prescribed. For example, requests for blood tests or the capture of ultrasound images. The definition of “intimate forensic procedures” can be found in section 23WA of the *Crimes Act 1914*.

Identifiers can be prescribed only if necessary for assisting in the identification, or authenticating the identity of a person seeking to sit a test (before making an application for citizenship by conferral under the general eligibility provisions); or of an applicant under the Act; or combating document or identity fraud in citizenship matters.

Definitions Section 3

“disclose, in relation to identifying information that is a personal identifier provided under Division 5 of Part 2, includes provide unauthorised access to the personal identifier.

Note: Section 42 deals with authorised access to identifying information.

‘Disclose’ means provide access to a personal identifier, whether the access is authorised or unauthorised.

entrusted person means:

- (a) the Secretary of the Department; or*
- (b) an APS employee in the Department; or*
- (c) a person engaged under section 74 of the Public Service Act 1999 by the Secretary of the Department; or*
- (d) a person engaged by the Commonwealth, the Minister, the Secretary of the Department, or by an APS employee in the Department, to do work for the purposes of this Act or the regulations or of the Migration Act 1958 or the regulations made under that Act.*

‘Entrusted person’ as defined includes all employees of the Department of

Immigration and Citizenship, whether they be ongoing, non-going or contracted staff, and people engaged to do work for the purposes of the Act or Regulations or the Migration Act or Regulations.

identifying information means the following:

- (a) any personal identifier provided under Division 5 of Part 2;
- (b) any meaningful identifier derived from any such personal identifier;
- (c) any record of a result of analysing any such personal identifier or any meaningful identifier derived from any such personal identifier;
- (d) any other information derived from:
 - (i) any such personal identifier; or
 - (ii) any meaningful identifier derived from any such personal identifier;or
 - (iii) any record of a kind referred to in paragraph (c);

that could be used to discover a particular person's identity or to get information about a particular person."

'Identifying information' is any personal identifier provided by an applicant for the purposes of the Act, and any additional information which can be used for identification purposes and is obtained either directly or indirectly from those personal identifiers.

If a personal identifier or any useful identifying information is analysed for any further information, the result of the analysis is also identifying information.

Any other information which is obtained through the further examination of a personal identifier or any of its derivatives, which can be used to confirm a person's identity or other information about that particular person, is identifying information.

DIVISION 5 OF THE ACT

Personal identifiers

Subdivision A – Obtaining personal identifiers

Request for personal identifiers Section 40

“(1) For the purposes of the Minister being satisfied of the identity of:

- (a) a person in relation to an application under this Part; or*
- (b) a person who has sought to sit a test approved in a determination under section 23A;*

the following persons may request the person, in writing, to provide one or more specified personal identifiers:

- (c) the Minister;*
- (d) a person authorised under subsection (3);*
- (e) a person who is included in a class of persons authorised under subsection (4).*

Form of request

(2) A request must inform the person of the matters prescribed by the regulations

Authorisations

(3) The Minister may, by writing, authorise a person for the purposes of paragraph (1)(d).

(4) The Minister may, by legislative instrument, authorise a class of persons for the purposes of paragraph (1)(e).”

A request may be made for one or more personal identifiers so that the Minister or delegate can be satisfied as to the identity of a person in relation to the sitting of a test (before making an application for citizenship by conferral under the general eligibility provisions), an application for citizenship or evidence of Australian citizenship.

When registering for a test, people will be required to either have a digital facial image taken by a Departmental officer or provide an appropriate photograph at the time of sitting the test.

All citizenship applicants (including those applying for evidence) 16 years and over, are required to provide an endorsed photograph and sign the application form as the specified personal identifiers.

A specific request for one or more personal identifiers under section 40 can only be made by a person delegated by the Minister under section 40.

Provision of personal identifiers Section 41

“The regulations may prescribe the procedures and requirements that apply to the provision of a personal identifier by a person under this Division.”

Regulation 11 Personal Identifiers, for subsection 40(2) of the Act, provides that a request must inform the applicant of the following matters:

“

- (a) why a personal identifier must be provided;*
- (b) how a personal identifier may be collected;*
- (c) how a personal identifier may be used;*
- (d) the circumstances in which a personal identifier may be disclosed to a third party;*
- (e) that a personal identifier may be produced in evidence in a court or tribunal in relation to the applicant who provided the personal identifier;*
- (f) that the Privacy Act 1988 applies to a personal identifier, and that the applicant has a right to make a complaint to the Privacy Commissioner about the handling of personal information;*
- (g) that the Freedom of Information Act 1982 gives a person access to certain information and documents in the possession of the Government of the Commonwealth and of its agencies, and that the applicant has a right under that Act to seek access to that information or those documents under that Act, and to seek amendment of records containing personal information that is incomplete, incorrect, out of date or misleading.”*

These matters have been included in all citizenship applications forms. Any other requests need to ensure that the matters are covered on each occasion a request is made.

Applicants sitting a test (before making an application for citizenship by

conferral under the general eligibility provisions) will be informed of these matters at the point of the registering for the test.

Subdivision B – Obligations relating to identifying information

Accessing identifying information Section 42

“(1) A person commits an offence if:

- (a) the person accesses identifying information; and*
- (b) the person is not authorised under this section to access the identifying information for the purpose for which the person accessed it.*

Penalty: Imprisonment for 2 years, or 120 penalty units, or both.

(1A) This section does not apply if the person believes on reasonable grounds that the access is necessary to prevent or lessen a serious and imminent threat to the life or health of the person or of any other person.

Note: A defendant bears an evidential burden in relation to the matter in subsection (1A) (see subsection 13.3(3) of the Criminal Code).

(2) This section does not apply if the access is through:

- (a) a disclosure that is a permitted disclosure within the meaning of section 43; or*
- (b) a disclosure to which section 43 does not apply because of the operation of subsection 43(1A).*

Note: A defendant bears an evidential burden in relation to the matter in subsection (2)(see subsection 13.3(3) of the Criminal Code).

Authorisation

(3) The Minister may, in writing, authorise a specified person, or any person included in a specified class of persons, to access identifying information of the kind specified in the authorisation.

(4) The Minister must specify in an authorisation under subsection (3), as the purpose or purposes for which access is authorised, one or more of the following purposes:

- (a) either or both of the purposes set out in paragraph 10(2)(c);*
- (b) disclosing identifying information in accordance with this Division;*
- (c) administering or managing the storage of identifying information;*
- (d) making identifying information available to the person to whom it relates;*
- (e) modifying identifying information to enable it to be matched with other identifying information;*
- (f) modifying identifying information in order to correct errors or ensure compliance with appropriate standards;*
- (g) the purposes of this Act or the regulations or of the Migration Act 1958 or the regulations made under that Act;*
- (h) complying with Australian laws.”*

Section 42 provides:

- that unauthorised access to identifying information is an offence and sets out the penalties for an offence;
- the circumstances in which personal identifiers can be lawfully accessed; and
- that the Minister may authorise specified people or classes of people to access identifying information.

Offences and Penalties

It is an offence for a person to access identifying information unless they are authorised to access the information for the purpose for which they have accessed it. The penalty is imprisonment for 2 years or 120 penalty units or both.

Authorised access

The offence provisions do not apply if:

- the access is for a purpose set out in subsection 42(4) and the person is authorised by the Minister to access the identifying information for that purpose; or
- there is reason to believe that access is necessary to prevent or lessen a serious and imminent threat to life or health of a person; or
- the access is for a disclosure that is a permitted disclosure under section 43 of the Act; or

- subsection 43(1A) applies.

Authorised by the Minister

People can be authorised by the Minister to access identifying information for the purposes set out in subsection 42(4). These purposes are intended to cover the circumstances in which people would need to access identifying information in the course of carrying out their duties as decision makers under the Act. Staff must establish that they have the required authorisation before accessing identifying information.

Serious and Imminent Threat to Life or Health

Any access of identifying information to prevent or lessen a serious threat to the life or health of a person may significantly disadvantage the person to whom the information relates. Consideration should therefore be given to whether there are any effective alternatives to accessing the identifying information.

The threatened harm must involve serious bodily injury, serious illness or death. The threat must be imminent or about to happen. The threat need not apply to a specific person. It may be a threat of serious harm to be randomly inflicted.

What is a ‘serious’ threat depends on the particular circumstances of each case. An explicit threat of murder or serious assault would usually be regarded as a serious threat, as would a threat of infection with a life-threatening condition. Threats of contracting (or being denied effective treatment for) a serious medical condition are regarded as threats to life or health. Abuse directed to staff in general does not usually count as a serious threat. Threats to finances or reputation are *not* threats to life or health.

Disclosing identifying information Section 43

“(1) A person commits an offence if:

- (a) the person’s conduct causes disclosure of identifying information; and*
- (b) the disclosure is not a permitted disclosure.*

Penalty: Imprisonment for 2 years, or 120 penalty units, or both.

(1A) If:

(a) a disclosure of identifying information is made to a person who is not an entrusted person; and

(b) the disclosure is a permitted disclosure;

this section does not apply in relation to any further disclosure of that identifying information by a person who is not an entrusted person.

Note 1: A defendant bears an evidential burden in relation to the matter in subsection (1A) (see subsection 13.3(3) of the Criminal Code).

Note 2: Paragraph 3 of Information Privacy Principle 11 in section 14 of the Privacy Act 1988 may apply to further disclosures of that identifying information by a person who is not an entrusted person.

(1B) This section does not apply if the person believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the person or of any other person.

Note: A defendant bears an evidential burden in relation to the matter in subsection (1B) (see subsection 13.3(3) of the Criminal Code).

(2) A **permitted disclosure** is a disclosure that:

(b) is for the purposes of this Act or the regulations or of the Migration Act 1958 or the regulations made under that Act; or

(c) is for the purpose of administering or managing the storage of identifying information; or

(d) is for the purpose of making the identifying information in question available to the person to whom it relates; or

(da) is to an agency of the Commonwealth, a State or a Territory in order to verify that a person is an Australian citizen; or

(e) takes place under an arrangement entered into with an agency of the Commonwealth, or with a State or Territory or an agency of a State or Territory, for the exchange of identifying information; or

(ea) is reasonably necessary for the enforcement of the criminal law of the Commonwealth, a State or a Territory; or

(eb) is required by an Australian law; or

- (f) *is for the purpose of a proceeding, before a court or tribunal, relating to the person to whom the identifying information in question relates; or*
- (g) *is for the purpose of an investigation by the Privacy Commissioner or the Ombudsman relating to action taken by the Department; or*
- (h) *takes place with the written consent of the person to whom the identifying information in question relates.”*

Section 43 provides that conduct causing disclosure of identifying information is an offence unless the disclosure is a permitted disclosure under subsection 43(2), and sets out the penalties for the offence. Section 43 also provides the following two exceptions to the offence provision:

- further disclosure by a person who is not an entrusted person but who obtained the information as a result of a permitted disclosure; and
- where the person believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health of a person.

Permitted Disclosure

Some of the permitted disclosures set out at subsection 43(2) above are self-explanatory. Further comment on others is set out below.

“(c) is for the purpose of administering or managing the storage of identifying information...”

This includes provision of identifying information to people employed by organisations providing file management and storage services to the Department.

“(d) is for the purpose of making the identifying information in question available to the person to whom it relates ...”

This includes, for example, complying with a request by an applicant or former applicant for information under the *Freedom of Information Act 1982*.

“(e) take place under an arrangement entered into with an agency of the Commonwealth, or with a State or Territory or an agency of a State or Territory ...”.

Currently there are no arrangements in place.

“(ea) is reasonably necessary for the enforcement of the criminal law of the Commonwealth, a State or a Territory ...”.

Policy is that there is a link between the proposed disclosure and the enforcement of the criminal law and that the link is strong enough to say that the use or disclosure is reasonably necessary to enforce the criminal law.

As a general rule, “reasonably necessary” implies that a disclosure need not be essential or critical to enforcing the criminal law. However, it must be more than just helpful, or of some assistance or expedient. In general, factors relevant to assessing this include:

- whether there are other practical and less intrusive measures available;
- whether the potential harm to the public interest in question is sufficiently strong to outweigh the privacy interests of the people in respect of whom the identifying information relates; and
- who is to receive the identifying information, and whether and how the identifying information is likely to be protected once it is disclosed.

Broadly speaking, criminal law encompasses those laws under which criminal proceedings can be initiated. These proceedings are usually initiated and prosecuted by the police or Crown prosecutors. They are usually heard in criminal courts, and may result in the accused being convicted and punished by fine or imprisonment.

Enforcing criminal law means the process of investigating crime and prosecuting criminals and the gathering of intelligence about crime to support the investigating and prosecuting functions of law enforcement agencies.

Identifying information reasonably necessary to the enforcement of the criminal law should be disclosed only to:

- an organisation that has statutory responsibilities for investigating or prosecuting criminal offences; or
- a person (or organisation) who require the identifying information to assist in the investigation or prosecution.

“(f) is for a purpose of a proceeding, before a court or tribunal, relating to the person to whom the identifying information in question relates ...”

The provision does not limit disclosure for the purpose of proceedings relating to the *Australian Citizenship Act 2007* but to proceedings involving the person to whom the identifying information relates.

“(g) is for the purpose of an investigation by the Privacy Commissioner or the Ombudsman relating to action taken by the Department ...”

An assessment should be made as to whether all identifying information held is or would be relevant to the investigation.

“(h) takes place with the written consent of the person to whom the identifying information in question relates.”

Written consent on an application form is only sufficient for disclosure for the purposes listed on the form.

Serious and Imminent Threat to Life or Health

Any disclosure of identifying information to prevent or lessen a serious threat to the life or health of a person may significantly disadvantage the person to whom the information relates. Consideration should therefore be given to whether there are any effective alternatives to accessing the identifying information.

The threatened harm must involve serious bodily injury, serious illness or death. The threat must be imminent or about to happen. The threat need not apply to a specific person. It may be a threat of serious harm to be randomly

inflicted.

What is a 'serious' threat depends on the particular circumstances of each case. An explicit threat of murder or serious assault would usually be regarded as a serious threat, as would a threat of infection with a life-threatening condition. Threats of contracting (or being denied effective treatment for) a serious medical condition are regarded as threats to life or health. Abuse directed to staff in general does not usually count as a serious threat. Threats to finances or reputation are *not* threats to life or health.

Unauthorised modification or impairment of identifying information Section 44

“Unauthorised modification

(1) *A person commits an offence if:*

- (a) the person causes any unauthorised modification of identifying information; and*
- (b) the person intends to cause the modification; and*
- (c) the person knows that the modification is unauthorised.*

Penalty: Imprisonment for 2 years, or 120 penalty units, or both.

Unauthorised impairment

(2) *A person commits an offence if:*

- (a) the person causes any unauthorised impairment of:*
 - (i) the reliability of identifying information; or*
 - (ii) the security of the storage of identifying information; or*
 - (iii) the operation of a system by which identifying information is stored; and*
- (b) the person intends to cause the impairment; and*
- (c) the person knows that the impairment is unauthorised.*

Penalty: Imprisonment for 2 years, or 120 penalty units, or both.

Exception

(2A) *If:*

- (a) a disclosure of identifying information is made to a person who is not an entrusted person; and
- (b) the disclosure is a permitted disclosure within the meaning of section 43;
this section does not apply in relation to any modification or impairment of that identifying information by a person who is not an entrusted person.

Note: A defendant bears an evidential burden in relation to the matter in subsection (2A) (see subsection 13.3(3) of the Criminal Code).

Interpretation

(3) In this section:

- (a) modification of identifying information; or
- (b) impairment of the reliability of identifying information; or
- (c) impairment of the security of the storage of identifying information; or
- (d) impairment of the operation of a system by which identifying information is stored;

by a person is **unauthorised** if the person is not entitled to cause that modification or impairment.

(4) Any such modification or impairment caused by the person is not unauthorised merely because he or she has an ulterior purpose for causing it.

(5) For the purposes of this section, a person causes any such unauthorised modification or impairment if the person's conduct substantially contributes to it.

(6) For the purposes of subsection (3), if:

- (a) a person causes any modification or impairment of a kind mentioned in that subsection; and
- (b) the person does so under a warrant issued under an Australian law;
the person is entitled to cause that modification or impairment.”

Section 44 provides that a person who is not authorised or entitled to modify identifying information, or impair the reliability of identifying information, or impair the security of the storage or the operation of a storage system of identifying information commits an offence if they:

- intentionally modify, or substantially contribute to the modification of identifying information; or
- intentionally impair, or substantially contribute to the impairment of, the reliability of identifying information, or the security of the storage of identifying information, or the operation of a storage system of identifying information; and
- know that their actions are unauthorised.

Modification or impairment is not unauthorised simply because the person has an ulterior motive for causing the modification or impairment.

Section 44 also provides the following exceptions to the offence provisions:

- modification or impairment of identifying information by a person who is not an entrusted person and received the identifying information as a result of a permitted disclosure (see above); and
- where the modification or impairment is done pursuant to a warrant issued under an Australian law.

'Modification' means changing or altering. For example:

- digitally altering a facial image so that it no longer looks like the person; or
- changing a person's signature so that it no longer has the characteristics of the person's signature.

The following actions are not considered to constitute modification:

- scanning a hard copy of a photograph to create a digital facial image; or
- cropping a photograph to enable it to be scanned; or
- photocopying a document containing a person's identifying information and blacking it out on the photocopy before disclosing the document to a third party (in accordance with the provisions of the Act and or the *Privacy Act 1988*, whichever is appropriate).

'Impairment' means damaging or weakening or making worse. For example:

- intentionally de-linking a facial image from a client record and connecting it to another person's identity information; or
- intentionally allowing another person to access a system storing identifying information that the other person is not authorised to access.

Destroying identifying information Section 45

“(1) A person commits an offence if:

- (a) the person is the responsible person for identifying information; and*
- (b) the person fails to destroy the identifying information as soon as practicable after the person is no longer required under the Archives Act 1983 to keep the identifying information.*

Penalty: Imprisonment for 2 years, or 120 penalty units, or both.

Note: See section 24 of the Archives Act 1983 on the obligation to keep the identifying information.

(2) This section does not apply if the identifying information is:

- (a) a personal identifier that is any of the following:*
 - (i) a measurement of a person’s height and weight;*
 - (ii) a photograph or other image of a person’s face and shoulders;*
 - (iii) a person’s signature; or*
- (b) identifying information derived from or relating to such a personal identifier.*

Note: A defendant bears an evidential burden in relation to the matters in subsection (2) (see subsection 13.3(3) of the Criminal Code).

Definitions

*(3) For the purposes of this section, the **responsible person** for identifying information is:*

- (a) if the identifying information is stored on a database—the person who has day-to-day control of the database; or*
- (b) otherwise - the person who has day-to-day responsibility for the system under which the identifying information is stored.*

*(4) For the purposes of this section, identifying information is **destroyed** if:*

- (a) in the case of identifying information that is a personal identifier—it is physically destroyed; and*
- (b) in any other case—any means of identifying it with the person to whom it relates is destroyed.*

*(5) For the purposes of this section, a **database** is a discrete body of information stored by electronic means, containing:*

- (a) indexes of persons who have provided personal identifiers in*

*accordance with a request under this Division; and
(b) their identifying information.”*

Section 45 provides that failure by the person responsible for identifying information to destroy the information as soon as possible after it is no longer required to be kept under the *Archives Act 1983* is an offence, **unless** the information is a measurement or a person’s height and weight, or a photograph or other image of a person’s face and shoulders, or a person’s signature, or information derived from or relating to those personal identifiers.

The person responsible for identifying information is the person who has:

- day-to-day control of the database, if the information is stored on a database; or
- day-to-day responsibility for the system under which the identifying information is stored.

A personal identifier is destroyed if it is physically destroyed, or any means of identifying it with the person to whom it relates is destroyed. For example, it is shredded, burned, deleted or erased so that it no longer exists, or it becomes illegible.

Retention and Storage of Identifying Information

The Act does not make provision for the indefinite retention of personal identifiers. The retention and disposal of identifying information is as required by the *Archives Act 1938* and as provided for by the relevant associated Department Records Disposal Authority.