5095/00/EN
WP40 final

Article 29 Data Protection Working Party

Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000

Adopted on 26th January 2001

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1]

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,
having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof

has adopted the following OPINION:

Introduction

Australia has had legislation covering the Commonwealth (federal) public sector since 1988 where the Privacy Act sets down detailed Information Privacy Principles (IPPs) based on the 1980 OECD Guidelines. The Privacy Act also applies to the private sector to the extent that it includes provisions and guidelines governing the consumer credit industry and restricting the use of tax file number information.[2] The Privacy Act created the Office of the Privacy Commissioner as a member of the Human Rights and Equal Opportunity Commission but since 1st July 2000, the Privacy Commissioner is established as a separate statutory agency.

The Privacy Amendment (Private Sector) Bill 2000 was passed by the Australian Parliament on 6 December 2000 and received Royal Assent on 21 December 2000. The new legislation contains amendments to the Commonwealth Privacy Act 1988 that will regulate the handling of personal information by private sector organisations. It will come into effect on 21 December 2001.

The Act implements the National Privacy Principles based on the National Principles for Fair Handling of Personal Information (NPPs) developed by the Federal Privacy Commissioner and released first in 1998 after extensive consultation with businesses and consumers. In the Act, the national principles provide a default framework setting out minimum standards in relation to how organisations should collect, use and disclose personal information. Private sector organisations are bound by the national principles unless they have their own privacy code that has been approved by the Privacy Commissioner. For ease of reference the National Principles are attached in annex 1.

Privacy Amendment (Private Sector) Act 2000

The working party welcomes the adoption of the Act and the work carried out in the past two years by the Privacy Commissioner, the Government and all interested parties which first led to the drafting of the National Principles for the Handling of Personal Information. It supports the Australian government goal to enhance the protection of personal data processed by the private sector and considers this work of great importance towards the fulfilment of Australia's commitment to abide by the 1980 OECD

[1] Official Journal no. L 281 of 23/11/1995, p. 31, available at:
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

[2] Other Commonwealth laws contain specific privacy provisions relating to information about health insurance claims, data matching, information about old criminal convictions and personal information disclosed by telecommunications companies (Telecommunications Act 1997)

guidelines. It recognises the innovative value s of the co-regulatory scheme which aims at bridging the gap between legislation and self-regulation by giving the latter the force of law.

From an European perspective, national data protection commissioners welcome developments that strengthen privacy protection in third countries as a means of meeting the requirements laid down in Articles 25 and 26 of the EU directive for data to flow to third countries. The working party also notes with interest it is possible for organisations to apply to the Privacy Commissioner to have a Privacy code approved which would operate in place of the standards in the legislation and that the Privacy Commissioner may only approve a code if it provides at least the same standard of privacy protection as the NPPs.

Sectors and activities excluded

The working party notes with concern that some sectors and activities are excluded from the protections of the Act. In particular:

Small business: only small businesses deemed to pose a high risk to privacy are required to comply with the legislation[3].

Moreover small business operators may choose to fall within the scope of the Act and to that effect notify their adherence to its provisions to the privacy Commissioner who keeps a register to that effect. Even though this possibility allows to identity the small business that voluntarily fall under the Act, the complexity of this exemption is such that it makes it very difficult to determine: a) what Australian business is a small business and b) whether or not it is exempt from the provisions of the Act.

The working party notes that this uncertainty renders it necessary to assume that all data transfers to Australian businesses are potentially to a small business operator which is not subject to the law, unless the name of the small business is inserted in the Privacy Commissioner's Register.

Employee data : An Act or practice engaged in by an organisation that is or was an employer of an individual is exempt from the Act if the act or practice is directly related to:

a) a current or former employment relationship between the employer and the individual, and
b) an employee record held by the organisation and relating to that individual

Employee records are defined in subsection 6 (1) in the broadest sense including information about the engagement, terms and conditions of contract, evaluative material over the performance of the contract, employee's emergency contacts, trade union membership, recreation long leave, taxation, banking affairs, etc.

---

[3] [3] These small businesses are identified in Section 6D of the Act as those that have an annual turnover of $3.000.000 or less and :

- provide a health service to another individual and hold health information except in an employee record, or
- collect from third parties or/and disclose personal information about another individual to third parties for a benefit, service or advantage unless the collection/disclosure is carried out with the individual's consent or as required or authorized by legislation or
- are contracted to provide a service to the Commonwealth

The working party notes that employee related data often contains sensitive data and sees no reason to exclude it at least from the protection given by NPP 10 for sensitive information. Moreover the exemptions allows information about previous employers to be collected and disclosed to a third party (eg a future employer) without the employee being informed.

It is the working party's opinion that the risk of privacy violations makes it all the more important to impose additional safeguards when exporting this type of data to Australia[4] and recommends that operators put into place appropriate means to do so (for example through contractual clauses).

Exceptions:

Exceptions to substantive data protection principles on the grounds that it is authorised by law:

National Privacy Principle NPP 2.1 (g) allows information to be used or disclosed for a secondary purpose where the use or disclosure is required or authorised by or under law[5].

In the working party's view it is acceptable to provide for an exception when organisations are faced with conflicting legal obligations, but to widen the exception to cover all options offered by sector specific laws, past present and future, risks undermining legal certainty and devoid the content of the basic protection. The wording "authorized" as opposed to "specifically authorized" which existed in the January 1999 edition of the National Principles can also be read to mean that all secondary purposes that are not forbidden are allowed. In the working party's view such a wide exemption would virtually devoid the purpose limitation principle of any value.

Publicly available data:

The collection of data for the purpose of including it in a generally available publication fall within the scope of NPPs1 (collection) but once the information is compiled in a format such that it comes within the definition of a generally available publication, the remaining Privacy Principles are not applied. This excludes all individual rights such as access and correction.

The working party notes that excluding publicly available personal data and in particular the secondary uses thereof from any protection is contrary to line taken by the directive. Moreover the 1980 OECD guidelines contain no such general exemption.

Transparency to data subjects:

NPP 1.3 (collection) allows for organisations to inform individuals before or at the time of collection but also adds that, if this is not practicable, it may inform individuals as soon as practicable thereafter.

---

[4] There is no exemption for employee records in the 1988 Privacy Act for the public sector.

[5] According to the Explanatory Memorandum page 119, the reference to "authorised *encompasses circumstances where the law permits, but does not require, use or disclosure"*. The reference to law (instead of legislation) is broad and may include any binding act.

The working party notes that allowing organisations to inform individuals after collection has been carried out is contrary to Principle 9 of the OECD Guidelines[6] This issue is of importance particularly with regard to sensitive data – where consent is one of the triggers for collection to be lawful in NPP 10.1.

Collection and use of data in particular with regard to direct marketing

NPPs 1 (collection) and 2 (use and disclosure) cover the purpose limitation principle by requiring collection of personal information to be necessary and by fair and lawful means[7], and by placing limits and conditions on use and disclosure.[8]

But the limitations with regard to use and disclosure concern only the secondary purpose. Processing for the 'primary' purpose of collection and 'related purposes within the reasonable expectation of the individual' are allowed provided that the individual has been given notice – consent is not required.

A practical result of this set up is that to use personal data for direct marketing it is not necessary to obtain the individual's consent (or respect any of the other limitations in NPP 2) if direct marketing is the primary purpose of collection. If instead it is the secondary purpose, opt-out must be provided every time the organisation sends the individual direct marketing material..
The working party recalls its opinion on "Transfers of personal data to third countries – WP 12" where it determined that allowing personal data to be used for direct marketing without an opt-out being offered cannot in any circumstance be considered adequate.

Sensitive data

National Privacy Principle 10 (sensitive information) places limitations only to the *collection of sensitive data.* There are no special restrictions or conditions on the use or disclosure of such data - other than health data, for which there are some provisions in NPP 2. The Act therefore allows most sensitive information which has been collected for a legitimate purpose to be used for other purposes subject only to the normal restrictions that apply to all types of data.

The working party notes that in the EU it is forbidden to process (i.e. collect, use and disclose) sensitive data unless one of a number of specific exemptions apply.

Lack of correction rights for EU citizens

Section 41 (4) allows the Privacy Commissioner to investigate an act or practice under NPP 6 or 7 only if it is an interference with the privacy of Australian citizens and the permanent residents. As a result, EU citizens that are no permanent residents in Australia but whose data was transferred from the EU to Australia may not exercise access and correction rights in relation to their data.

Onward transfers from Australia to other third countries

[6] « The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose »
[7] Privacy Amendment (Private Sector) Act 2000, Schedule 3, NPP1.1 & 1.2
[8] Privacy Amendment (Private Sector) Act 2000, Schedule 3, NPP2

NPP 9 prohibits exports of personal information by an organisation to someone in a foreign country (other than an affiliate of the organisation itself) unless one of six conditions applies.

With reference to NPP 9 (a) : (applicable when recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles) the working party is of the opinion that the assistance of the Privacy Commissioner in indicating what third country regime can be considered as substantially similar to the Australian domestic situation is advisable.

With reference to NPP 9(f): (which applies when all the other five conditions are not applicable, hence when the recipient is not subject to a law, binding scheme or contract) the working party notes that this provision does not take into account the individuals' right to see his rights enforced.Moreover, the working party notes that Section 5 on the extra territorial operation of the Act, applies only to Australians and *does not extend the protection of NPP9 to non-Australians.* This means that an Australian company can import data from European citizens and subsequently export it to a country with no privacy laws without the Australian Act applying. Such a measure would make it possible to circumvent the EU Directive, if Australia was recognised as providing adequate protection.

Conclusions

On the basis of the above, the working party considers that data transfers to Australia could be regarded as adequate only if appropriate safeguards were introduced to meet the above mentioned concerns. This could be done for example through voluntary codes of conduct foreseen in Part IIIAA of the Act taking into account that the enforcement of voluntary codes is done either by the Privacy Commissioner himself or by an independent adjudicator.

But with a view to obtain a more comprehensive adequacy assessment, the working party encourages the Commission to continue to follow the issue to seek improvements of general application and to keep the Working Party informed of developments.

Brussels, 26 January 2000

National Privacy Principles (annexed to the Privacy Amendment (Private Sector) Act 2000

1 Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2 Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose of collection unless:

(a) both of the following apply:

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

(i) it is impracticable for the organisation to seek the individual's consent before that particular use; and

(ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(iii) the individual has not made a request to the organisation not to receive direct marketing communications; and

(iv)in each direct marketing communication with the individual , the organisation draws to the individual’s attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications ; and

(v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation’s business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically or

(d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and

(iii) in the case of disclosure-the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

(e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or

(ii) a serious threat to public health or public safety; or

(f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(g) the use or disclosure is required or authorised by or under law; or

(h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause. 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

(a) the individual:

(i) is physically or legally incapable of giving consent to the disclosure; or

(ii) physically cannot communicate consent to the disclosure; and

(b) a natural person (the ***carer***) providing the health service for the organisation is satisfied that either:

(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(c) the disclosure is not contrary to any wish:

(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

(d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is ***responsible*** for an individual if the person is:

(a) a parent of the individual; or

(b) a child or sibling of the individual and at least 18 years old; or

(c) a spouse or de facto spouse of the individual; or

(d) a relative of the individual, at least 18 years old and a member of the individual's household; or

(e) a guardian of the individual; or

(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or

(g) a person who has an intimate personal relationship with the individual; or

(h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:
child of an individual includes an adopted child, a step-child and a foster-child, of the individual.
parent of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.
relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.
sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

3 Data quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

4 Data security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

5 Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6 Access and correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

(a) in the case of personal information other than health information-providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) in the case of health information-providing access would pose a serious threat to the life or health of any individual; or

(c) providing access would have an unreasonable impact upon the privacy of other individuals; or

(d) the request for access is frivolous or vexatious; or

(e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(g) providing access would be unlawful; or

(h) denying access is required or authorised by or under law; or

(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) providing access would be likely to prejudice:
(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or
(iii) the protection of the public revenue; or
(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;
by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, those charges:
(a) must not be excessive; and
(b) must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7 Identifiers

7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:
(a) an agency; or

(b) an agent of an agency acting in its capacity as agent; or

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, sub-clause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identified in prescribed circumstances.

Note : There are prerequisites that must be satisfied before those matters are prescribed (see subsection 100 (2)).

7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or

(b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure, or

(c)the use or disclosure is by a prescribed organisation of a prescribed identified in prescribed circumstances

Note : There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsection 100 (2)

7.3 In this clause:
identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's nameor ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*is not an ***identifier***.

8 Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9 Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply:
(i) the transfer is for the benefit of the individual;
(ii) it is impracticable to obtain the consent of the individual to that transfer;
(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or
(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

10 Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required by law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:
(i) is physically or legally incapable of giving consent to the collection; or
(ii) physically cannot communicate consent to the collection; or
(d) if the information is collected in the course of the activities of a non-profit organisation-the following conditions are satisfied:
(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;
(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or
(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:
(a) the information is necessary to provide a health service to the individual;
and
(b) the information is collected:
(i) as required by law (other than this Act); or
(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:
(a) the collection is necessary for any of the following purposes:
(i) research relevant to public health or public safety;
(ii) the compilation or analysis of statistics relevant to public health or public safety;
(iii) the management, funding or monitoring of a health service; and
(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and
(c) it is impracticable for the organisation to seek the individual's consent to the collection; and
(d) the information is collected:
(i) as required by law (other than this Act); or
(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or
(iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:
non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims

Done at Brussels, 26th January 2001

For the Working Party

The Chairman

Stefano RODOTA