FIRST PRINT

DATA PROTECTION BILL 1991

NEW SOUTH WALES

EXPLANATORY NOTE

(This Explanatory Note relates to this Bill as introduced into Parliament)

The objects of this Bill are:

(a) to prohibit individuals from releasing government data for individual financial gain; and

(b) to provide appropriate mechanisms for the implementation of data protection safeguards in both the public and private sectors; and

(c) consequently to confer data protection functions on the Privacy Committee.

PART 1—PRELIMINARY

Clause 1 specifies the short title of the proposed Act.

Clause 2 provides that the proposed Act commences on assent.

Clause 3 sets out the objects of the proposed Act.

Clause 4 defines expressions used in the proposed Act.

Clause 5 provides that the Act binds the Crown but makes it clear that the Crown will not be liable to be prosecuted for an offence.

PART 2—CORRUPT DEALINGS WITH PUBLIC SECTOR INFORMATION

Clause 6 prohibits a public employee or former public employee from using or disclosing personal information gained in the performance of official functions for the purpose of obtaining a financial or other benefit. The maximum penalty for the offence will be 100 penalty units (currently $10,000) or 2 years imprisonment, or both.

Clause 7 prohibits a person from giving or offering to give a financial or other benefit to a public employee or former public employee (or attempting to do so) in return for the disclosure of personal information. The maximum penalty for the offence will be 100 penalty units (currently $10,000) or 2 years imprisonment, or both.

Clause 8 prohibits a person from obtaining personal information that the person knows, or ought reasonably to know, was disclosed in contravention of proposed section 6. The maximum penalty for the offence will be 100 penalty units (currently $10,000) or 2 years imprisonment, or both.

Clause 9 prohibits a person from offering to supply or holding himself or herself out as being able to supply personal information that the person knows, or ought reasonably to know, has been or is proposed to be disclosed in contravention of proposed section 6. The maximum penalty for the offence will be 100 penalty units (currently $10,000) or 2 years imprisonment, or both.

Clause 10 makes it clear that a public employee acting in the exercise of official functions, or a person who lawfully obtains personal information, will not be guilty of an offence under proposed section 6, 7, 8 or 9.

PART 3—DATA PROTECTION SAFEGUARDS

Division 1—Codes of practice

Clause 11 requires heads of government Departments and State authorities to prepare codes of practice for the use and disclosure of, and procedures for dealing with, personal information. The codes must be prepared not later than 12 months after the commencement of the proposed Act.

Clause 12 sets out the requirements for such codes. The codes are to be in accordance with the data protection principles set out in proposed Division 3.

Clause 13 enables a Department Head or chief executive to exempt information or persons from codes of practices, after submitting proposed exemptions to the Privacy Committee and consideration of any representations made by the Privacy Committee.

Clause 14 provides that the Privacy Committee may prepare, or review, codes of practice relating to personal information held in the private sector.

Clause 15 sets out the requirements for codes prepared by the Privacy Committee and the matters to be taken into account by the Committee in reviewing a code.

Division 2—Functions of the Privacy Committee

Clause 16 confers additional functions relating to data protection on the Privacy Committee.

Division 3—Data protection principles

Clause 17 sets out the data protection principles.

PART 4—MISCELLANEOUS

Clause 18 provides that offences against the proposed Act are to be dealt with summarily before a Local Court constituted by a Magistrate sitting alone.

Clause 19 requires the Privacy Committee to report to the Minister on the proposed Act not later than 2 years after the proposed Act commences. The Minister must then lay the report before both Houses of Parliament.

FIRST PRINT

DATA PROTECTION BILL 1991

NEW SOUTH WALES

TABLE OF PROVISIONS

DATA PROTECTION BILL 1991

NEW SOUTH WALES

No. , 1991

A BILL FOR

An Act to make provision for data protection safeguards in connection with records and to prohibit individuals from releasing government data for financial gain.

The Legislature of New South Wales enacts:

PART 1—PRELIMINARY

Short title

1. This Act may be cited as the Data Protection Act 1991.

Commencement

2. This Act commences on the date of assent to this Act.

Objects

3. The objects of this Act are to prohibit individuals from releasing government data for individual financial gain, to provide appropriate mechanisms for the implementation of data protection safeguards in both the public and private sectors and consequently to confer data protection functions on the Privacy Committee.

Definitions

4. (1) In this Act:

"benefit" includes advantage;

"Department Head" has the same meaning as in the Public Sector Management Act 1988;

"judicial officer" has the same meaning as in the Judicial Officers Act 1986;

"local government authority" means a council of a city, municipality or shire, a county council, an urban committee or a person exercising all or any of the functions of such a council or committee;

"personal information" means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion;

"Privacy Committee" means the Privacy Committee established under the Privacy Committee Act 1975;

"public employee" means any of the following persons:

(a) a person appointed by the Governor or a Minister of the Crown to a statutory office;

(b) a person employed in the Public Service, the Education Teaching Service or the Police Service;

(c) a person who is an officer of the Legislative Council or Legislative Assembly or who is employed by (or under the control of) the President of the Legislative Council or the Speaker of the Legislative Assembly, or both;

(d) a person who is employed by (or engaged as a consultant by) the State, an authority of the State, a local government authority or a public employee;

(e) a person who acts for or on behalf of or in the place of or as deputy or delegate of an authority of the State, a local government authority or a public employee,

but does not include the Governor, a Minister of the Crown, a member of Parliament, a local government member or a judicial officer.

(2) In this Act:

(a) a reference to a function includes a reference to a power, authority and duty; and

(b) a reference to the exercise of a function includes, if the function is a duty, a reference to the performance of a duty.

Crown bound by this Act

5. (1) This Act binds the Crown not only in right of New South Wales but also, in so far as the legislative power of Parliament permits, the Crown in all its other capacities.

(2) Nothing in this Act renders the Crown liable to be prosecuted for an offence.

PART 2—CORRUPT DEALINGS WITH PUBLIC SECTOR INFORMATION

Use and disclosure of information

6. A public employee or former public employee must not, for the purpose of obtaining a financial or other benefit (whether for the employee or former employee or for any other person), use or disclose any personal information to which the employee or former employee has or had access in the performance of his or her official functions.

Maximum penalty: 100 penalty units or imprisonment for 2 years, or both.

Soliciting disclosure of information

7. A person who gives, or offers to give, or attempts to give or offer to give, a financial or other benefit to a public employee or former public employee in consideration of the disclosure by the employee or former employee of personal information to which the employee or former employee has or had, or may have or have had, access in the performance of his or her official functions is guilty of an offence.

Maximum penalty: 100 penalty units or imprisonment for 2 years, or both.

Obtaining information

8. A person who obtains personal information that the person knows, or ought reasonably to know, was disclosed by a public employee in contravention of section 6 and who uses or discloses the information to another person is guilty of an offence.

Maximum penalty: 100 penalty units or imprisonment for 2 years, or both.

Offering to supply information

9. A person who offers to supply (whether to a particular person or otherwise), or holds himself or herself out as being able to supply (whether to a particular person or otherwise), personal information that the person knows, or ought reasonably to know, has been or is proposed to be disclosed in contravention of section 6 is guilty of an offence.

Maximum penalty: 100 penalty units or imprisonment for 2 years, or both.

Protection of public employees etc.

10. (1) Nothing in this Part renders a public employee acting in the exercise of his or her official functions guilty of an offence.

(2) Nothing in this Part renders a person who is permitted by law to obtain personal information, whether or not on payment of a fee, guilty of an offence for obtaining personal information in accordance with that law.

PART 3—DATA PROTECTION SAFEGUARDS

Division 1—Codes of practice

Duty of heads of government Departments etc.

11. (1) For the purpose of better protecting individual privacy, each Department Head, and each chief executive officer of an authority of the State, is to prepare a code of practice relating to the use and disclosure, and procedures for dealing with, personal information held by the Department or administrative office or authority, as the case may be, administered by the Department Head or chief executive officer.

(2) The code of practice must be prepared not later than 12 months after the commencement of this Act.

Requirements for public sector codes of practice

12. (1) A code of practice must:

(a) classify personal information held by the Department or administrative office or authority concerned according to degrees of confidentiality; and

(b) specify procedures for dealing with any such information with a view to safeguarding its confidentiality.

(2) The code must generally conform to the data protection principles set out in Division 3.

Exemptions

13. (1) A Department Head or chief executive officer required by section 11 to prepare a code of practice may exempt personal information or classes of personal information or a person or any classes of persons from any or all of the provisions of the code.

(2) Before exempting information or a person or a class of information or persons, the Department Head or chief executive officer must refer the proposed exemption to the Privacy Committee and consider any representations made by the Privacy Committee as to the proposed exemption.

Private sector codes of practice

14. The Privacy Committee may, at the request of a person or group of persons, prepare or review a code of practice relating to personal information held by the person or group of persons and procedures for dealing with that personal information.

Requirements for review and preparation of private sector codes of practice

15. (1) In preparing a code of practice under this Division, the Privacy Committee must:

(a) classify personal information held by persons to whom the code applies according to degrees of confidentiality; and

(b) specify procedures for dealing with any such information with a view to safeguarding its confidentiality.

(2) The code must generally conform to the data protection principles set out in Division 3.

(3) In reviewing a code of practice, the Privacy Committee is to have regard to the matters set out in subsections (1) and (2).

Division 2—Functions of the Privacy Committee

Functions of the Privacy Committee

16. (1) The Privacy Committee has the following functions:

(a) to promote the adoption of, and compliance with, data protection principles in both the public and private sectors;

(b) to conduct research into any matter relating to data protection;

(c) to prepare and publish guidelines in relation to data protection;

(d) to provide advice to any person, and to prepare and publish reports and recommendations, concerning the need for, or the desirability of, legislative, administrative or other action in the interest of the privacy of persons;

(e) to monitor developments in technology which may have an adverse impact on data protection and report on how any adverse impact may be minimised;

(f) to receive and investigate complaints about the use and disclosure of personal information, and for that purpose, to conduct such inquiries and make such investigations as it thinks fit;

(g) to make reports to complainants;

(h) to prepare and publish a personal information digest.

(2) These functions are in addition to any other functions conferred on the Privacy Committee by or under this or any other Act.

(3) For the purposes of exercising its functions under subsection (1) (f), the Privacy Committee has the functions conferred on it by section 16 of the Privacy Committee Act 1975.

Division 3—Data protection principles

Data protection principles

17. The data protection principles are as follows:

Principle 1

Manner and purpose of collection of information

1. Personal information must not be collected by a collector for inclusion in a record or in a generally available publication unless:

(a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and

(b) the collection of the information is necessary for or directly related to that purpose.

2. Personal information must not be collected by a collector by unlawful or unfair means.

Principle 2

Solicitation of information from individual concerned

1. Personal information must be solicited directly from the individual concerned except where the individual authorises otherwise, or where information may be disclosed to the collector in accordance with these principles or a code of practice under this Act.

2. Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector from the individual concerned,

the collector must take such steps (if any) as are, in the circumstances, reasonable to ensure that, before the information is collected (or, if that is not practicable, as soon as practicable after the information is collected) the individual concerned is informed of:

(c) the purpose for which the information is being collected; and

(d) if the collection of the information is authorised or required by or under law—the fact that the collection of the information is so authorised or required; and

(e) the mandatory or voluntary nature of the information collection and the effects on the individual concerned (if any) of not providing all or any part of the requested information; and

(f) the existence of the right of access to and rectification of the data relating to the individual; and

(g) the name and address of the recordkeeper; and

(h) any person to whom, or any body or agency to which, it is the collector's usual practice to disclose information of the kind so collected, and (if known by the collector) any person to whom, or any body or agency to which, it is the usual practice of that first mentioned person, body or agency to pass on that information.

Principle 3

Solicitation of information generally

Where:

(a) a collector collects personal information for inclusion in a record or in a generally available publication; and

(b) the information is solicited by the collector,

the collector must take such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is collected:

(c) the information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete; and

(d) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual concerned.

Principle 4

Storage and security of information

A recordkeeper who has possession or control of a record that contains personal information must ensure that the information is:

(a) stored for specified, explicit and lawful purposes and used in a way consistent with those purposes; and

(b) adequate, relevant, and not excessive in relation to the purposes for which it is stored; and

(c) processed fairly and lawfully; and

(d) kept for no longer than is necessary for the purposes for which the information is stored; and

(e) protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse,

and if it is necessary for the information to be given to a person in connection with the provision of a service to the recordkeeper, everything reasonably within the power of the recordkeeper is done to prevent unauthorised use or disclosure of the information.

Principle 5

Information relating to records kept by recordkeeper

1. A recordkeeper who has possession or control of records that contain personal information must, subject to clause 2 of this Principle, take such steps as are, in the circumstances, reasonable to enable any person to ascertain:

(a) whether the recordkeeper has possession or control of any records that contain any such information; and

(b) whether the recordkeeper has possession or control of such a record relating to that person; and

(c) if the recordkeeper has possession or control of a record that contains such information:

(i) the nature of that information; and

(ii) the main purposes for which the information is used; and

(iii) the steps that the person should take if the person wishes to obtain access to the record.

2. A recordkeeper is not required under clause 1 of this Principle to give a person information if the recordkeeper is required or authorised to refuse to give that information to the person under the applicable provision of any law of New South Wales that provides for access by persons to documents.

3. A recordkeeper must maintain a record setting out:

(a) the nature of the records of information about individuals kept by or on behalf of the recordkeeper; and

(b) the sources of information contained in those records; and

(c) the purpose for which the information was collected and the authority for that collection; and

(d) the purpose for which each type of record is kept; and

(e) the classes of individuals about whom records are kept; and

(f) the period for which each type of record is kept; and

(g) the persons who are entitled to have access to information about individuals contained in the records and the conditions under which they are entitled to have that access; and

(h) the steps that should be taken by persons wishing to obtain access to that information.

4. A recordkeeper must:

(a) make the record maintained under clause 3 of this Principle available for inspection by members of the public; and

(b) give the Privacy Committee, in the month of June in each year, a copy of the record so maintained.

Principle 6

Access to records containing information about individuals

Where a recordkeeper has possession or control of a record that contains personal information, the individual concerned is, without excessive delay or expense, entitled to have access to that record, except to the extent that the recordkeeper is required or authorised to refuse to provide the individual with access to that record under the applicable provision of any law of New south Wales that provides for access by persons to documents.

Principle 7

Alteration of records containing information about individuals

1. A recordkeeper who has possession or control of a record that contains personal information must take such steps (if any), by way of making appropriate corrections, deletions and additions as are, in the circumstances, reasonable to ensure that the record:

(a) is accurate; and

(b) is, having regard to the purpose for which the information was collected or is to be used and to any purpose that is directly related to that purpose, relevant, up to date, complete and not misleading.

2. Where personal information has been corrected, deleted or added to in accordance with clause 1, the individual concerned is entitled to have recipients of that information notified of the alterations by the recordkeeper.

3. The obligation imposed on a recordkeeper by clause 1 is subject to any applicable limitation in a law of New South Wales that provides a right to require the correction or amendment of documents.

4. Where:

(a) the recordkeeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned; and

(b) no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of New South Wales,

the recordkeeper must, if so requested by the individual concerned, take such steps (if any) as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Principle 8

Recordkeeper to check accuracy etc. of information before use

A recordkeeper who has possession or control of a record that contains personal information must not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date and complete.

Principle 9

Limits on use of information

A recordkeeper who has possession or control of a record that contains personal information must not use the information for a purpose other than that for which it was collected and which was specified in accordance with Principle 5 unless:

(a) the individual concerned has consented to use of the information for that other purpose; or

(b) the recordkeeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person; or

(c) use of the information for that other purpose is required or authorised by or under law.

Principle 10

Limits on disclosure of information

1. A recordkeeper who has possession or control of a record that contains personal information must not disclose the information to a person, body or agency (other than the individual concerned) unless:

(a) the individual concerned has been informed under Principle 2 that information of that kind is usually passed to that person, body or agency; or

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

(c) the recordkeeper 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 individual concerned or of another person; or

(d) the disclosure is required or authorised by or under law.

2. A person, body or agency to whom information is disclosed under clause 1 of this Principle must not use or disclose the information for a purpose other than the purpose for which the information was given to the person, body or agency.

Principle 11

Limits on use of certain information

1. Despite Principles 9 and 10, information relating to ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life must not be used or disclosed by a recordkeeper without the express written consent, freely given, of the individual concerned, except to the extent that the recordkeeper is required or authorised to do so under the law of New South Wales.

2. Information relating to an individual's criminal history may only be processed as required or authorised by law or a code of practice under this Act.

PART 4—MISCELLANEOUS

Proceedings for offences

18. Proceedings for an offence against this Act are to be dealt with summarily before a Local Court constituted by a Magistrate sitting alone.

Report on legislation

19. (1) The Privacy Committee must, not later than 2 years after the commencement of this Act, prepare and submit to the Minister a report as to the operation of this Act.

(2) The Minister must, as soon as practicable after receiving the report, lay the report or cause it to be laid, before both Houses of Parliament.