EU Working Party Issues Opinions on Australian and Canadian DP Laws

THE ARTICLE 29 DATA PROTECTION WORKING PARTY has issued opinions on the adequacy of the Australian Privacy Amendment (Private Sector) Act 2000 and Canada's Personal Information Protection and Electronic Documents Act. Both opinions were adopted on January 26th, 2001.

AUSTRALIA

The Privacy Amendment (Private Sector) Act 2000 (PL&B Feb 2001 p.10) was passed by Parliament on December 6th 2000 and will come into effect on December 21st 2001.

The Working Party raised many concerns about the new legislation, which will regulate the handling of personal information by private sector organisations.

EXCLUDED SECTORS

The Working Party was concerned that some sectors and activities are excluded from the Act. These are:

1. Small business

Only small businesses deemed to pose a high risk to privacy are required to comply with the legislation. The Act creates a voluntary compliance program for small businesses. The complexity of this exemption makes it very difficult to determine: a) what is a small business and b) whether it is exempt from the Act. The Working Party said it was therefore 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.

2. 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.

The Working Party noted that employee-related data often contains sensitive data and saw no reason to exclude it at least from the protection given by National Privacy Principle (NPP) 10 for sensitive information. Moreover, the exemption allows information about previous employers to be collected and disclosed to a third party (for example, a future employer) without the employee being informed.

The Working Party advised that the risk of privacy violations makes it all the more important to impose additional safeguards when exporting this type of data to Australia. It recommended that operators put into place appropriate means to do so (for example, contractual clauses).

SECONDARY USES AND DISCLOSURES

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. The Working Party agreed that it was 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 deprive 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 NPP s1 (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 noted that excluding publicly available personal data, and in particular the secondary uses, from any protection is contrary

to the position taken by the Directive.

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. The Working Party noted that allowing organisations to inform individuals after collection has been carried out is contrary to Principle 9 of the OECD Guidelines. This is of particular importance with sensitive data.

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, and by placing limits and conditions on use and disclosure.

However, 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, and is therefore not necessary for direct marketing. Nor is it necessary to respect any of the other limitations in NPP 2 if direct marketing is the primary purpose of collection.

The Working Party recalled its opinion on "Transfers of personal data to third countries – WP 12". There, it determined that allowing personal data to be used for direct marketing without offering an opt-out cannot in any circumstance be considered adequate.

Sensitive data

NPP 10 (sensitive information) places limitations only on collecting 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 noted that in the EU it is forbidden to process sensitive data unless one of a number of specific exemptions apply.

Lack of correction rights for EU citizens

The Act 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 permanent residents. As a result, EU citizens who are not permanent residents in Australia but whose data was transferred from the EU to Australia may not exercise access and correction rights.

Onward transfers from Australia to other third countries

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.

Among the concerns was 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. If Australia was recognised as providing adequate protection, such an import-export measure would make it possible to circumvent the EU Directive.

Recommendations

The Working Party concluded that data transfers to Australia could be regarded as adequate only if appropriate safeguards were introduced to meet the concerns mentioned above. 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.

To obtain a more comprehensive adequacy assessment, the Working Party encouraged the Commission to continue to follow the issue to seek improvements of general application.

Canada

Still Some Gaps

The Working Party has given what appears to be qualified support for finding of adequacy for the Personal Information Protection and Electronic Documents Act, which came into force in part on January 1st 2001 (PL&B July 00 p.3, Feb 01 p.3).

Sensitive data

The Working Party notes that the Act does not identify sensitive data as such. Data is regarded as sensitive depending on the context in which it is used. There is no prohibition on the collection of sensitive data. The Working Party noted, however, that clauses in the Schedule to the Act call for greater protection of sensitive information and impose more stringent consent requirements for sensitive information.

The Working Party said it would "welcome the systematic use of highest level of protection when sensitive data is processed." It encouraged the Canadian authorities and in particular the Federal Privacy Commissioner to work towards this goal.

Health information

The Working Party noted that most of the health information in private organisations will not be covered by the Act until 2004, when the Act applies to provincial organisations in

the commercial sector. That is where most such information is found.

Employee data

The Working Party noted that employee data exported from the EU to Canada falls under the Act as of January 1st 2001, if the data is about an employee of Canadian federally related undertakings, such as railways and banks, or if the exchange of information is carried out for a commercial purpose. However, there is uncertainty about the Act's coverage of employee information in organisations outside Federal jurisdiction, ie. organisations regulated by provincial law. There may be a difference in interpretation between the Working Party and the book written by Perrin, Black et al on Bill C-6 (see Book Review p.22). The book states, (p. 59) that employee information other than that in connection with a federal work is not covered by the Act. They argue that, contrary to the position apparently taken by the Working Party, employee information, labour relations etc. is not counted within the meaning of "commercial", and is therefore not subject to the Act.

Transfers outside Canada

The Working Party concluded that the transfer of data outside Canada would require the use of contractual or other binding provisions able to provide a comparable level of protection. It encouraged the Canadian authorities to issue guidance to this effect.

Recommendations

The Working Party recommended that any adequacy finding for the Personal Information and Electronic Documents Act reflects the limitations in scope and the implementation timetable. It noted two limitations in particular. The Act applies only to private sector organisations that collect, use or disclose personal information in the course of commercial activities. Moreover, the Act will enter into force in three stages, with full implementation occurring only in 2004.

The Working Party also invited the Commission and the Art. 31 Committee to look into the process leading to the definition of "substantially similar" legislation. (The private sector data protection activities under provincial jurisdiction will be exempted from the Act if the provinces enact legislation that is "substantially similar" to the federal Act to cover those activities).

The Working Party also invited the Commission to follow the process with regard to health data and encouraged initiatives to foster coherent and comprehensive rules throughout Canada.

Finally the Working Party "welcomed any initiative on the part of the Canadian authorities to provide the highest possible protection for sensitive data and ensure that a comparable level of protection is provided for when data is transferred from Canada to another country."

The Working Party opinions on Canada (DG MARKT 5095/00) and Australia (DG MARKT 5001/01) can be found at the following website: http://www.europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm