ARTICLE 29 DATA PROTECTION WORKING PARTY

00665/11/EN
WP 182

Opinion 11/2011 on the level of protection of personal data in New Zealand

Adopted on 4 April 2011

The Working Party on the protection of individuals with regard to the processing of personal data

Having regard to Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and in particular Articles 29 and 30 paragraph 1 (b) thereof,

having regard to the Rules of Procedure of the Working Party, and in particular Articles 12 and 14 thereof,

has adopted the following opinion.

1. Introduction and background

The Working Party was requested to consider the adequacy of New Zealand data protection legislation in 2009 and the relevant subgroup was given this mandate at the December 2009 plenary.

The European Commission provided a report it had requested on the adequacy of the protection of personal data in New Zealand, which was written by Professor Roth, Faculty of Law, University of Otago, Dunedin, New Zealand. This report was written under the supervision of the Centre de Recherches Informatique et Droit (CRID) of the University of Namur. The report analyses the degree to which the New Zealand legal system complies with requirements in terms of substantive legislation and the implementation of mechanisms to apply regulations protecting personal data, set out in the working paper "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive", approved by the Article 29 Working Party on 24 July 1998 (WP 12). It also takes account of non-legal rules, application in practice, and the general administrative and corporate culture that exists in relation to privacy.

The subgroup considered this report as well as the comments on this report from the NZ DPA, the NZ Ministry of Justice, and the letter from the Ministry of Justice regarding the Privacy (Cross-border Information) Amendment Act 2010. The subgroup also asked the New Zealand Privacy Commissioner (the national supervisory authority) for further information and clarification on some aspects, which are set out below. The subgroup then considered the information received, which included guidance from the Privacy Commissioner on the application of the Privacy (Cross-border Information) Amendment Act following its entry into force on 7 September 2010.

This opinion draws heavily on Professor Roth's report, which was clearly written and helpfully structured to consider New Zealand legislation against each of the requirements in WP 12.

2. Legislation on data protection in New Zealand

New Zealand does not have a written constitution and is a Parliamentary democracy. There are a number of statutes that have constitutional significance and are regarded as 'higher law'. These include the New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993. There are also a number of common law principles and rules relevant to data protection including the recognition of common law torts for privacy as well as breach of confidence.

The main data protection legislation in New Zealand is the Privacy Act 1993 (the Act), which was heavily influenced by the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. There are three full privacy codes of practice made under section 46 of the

Act that apply specifically, and with more stringent standards, to health information, telecommunications information, and credit reporting information. There are also laws relating to areas such as freedom of information; spam; criminal law sanctions for certain breaches of privacy; spent criminal convictions; surveillance; the retention of health information; public records; and discrimination law. There are also privacy-related provisions in other legislation, for example, secrecy provisions in the Electoral Act 1993 that protect the privacy of the voter.

The Privacy Act establishes the office of Privacy Commissioner as an independent entity. The Privacy Commissioner has issued various guidelines, factsheets and other information to set out rights and obligations for organisations and individuals, as well as anonymised case notes relating to specific complaints. These provide guidance on the practical application of privacy principles. In addition, human rights case law has provided guidance and interpretation on aspects of the Privacy Act.

New Zealand also has two statutes relating to freedom of information that contain privacy provisions. The Official Information Act covers central government and public sector agencies; the Local Government Official Information and Meetings Act 1987 covers local government. There are privacy provisions for when government information is proposed to be disclosed, and the right to reasons for government decisions that affect individuals.

New Zealand has an independent judiciary and Privacy Act cases can be brought before the Human Rights Review Tribunal. The District Court considers common law and criminal law matters. Appeals from both these courts are heard in the High Court. Above this court are a Court of Appeal and then a Supreme Court.

There are civil remedies that relate to privacy, including defamation, nuisance, harassment, malicious falsehood, trespass, intentional infliction of harm, negligence, and passing off. In addition under criminal law there are various offences relating to intrusion into an individual's privacy, which include the unauthorised use or disclosure of personal information.

Finally, it is relevant that New Zealand is a small country of approximately 4.3 million people and as the expert report makes clear fair information handling is seen as good business. Organisations cannot afford to alienate such a small market, and news of poor practice spreads quickly. This has a significant effect on business practice.

3. Assessment of the level of adequacy of data protection afforded by the legislation in New Zealand

The Working Party points out that its assessment on the adequacy of the law on data protection in New Zealand focuses on the Privacy Act 1993.

This Act's provisions, as well as the case law made by the courts with regard to the protection of personal data, have been compared with the main provisions of the Directive, taking into account opinion WP 12 of the Working Party. This opinion lists a number of principles which constitute "*a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate*."

3.1. Scope of application of the legislation

The Act covers all personal information in whatever shape or form. It covers the entire public and private sectors, with a few specific public interest exceptions as is usual in a democratic society.

The Act defines personal information as "*information about an identifiable individual*", where the individual is a living natural person, and it includes information relating to a death on the official register of deaths.

With regard to identifiability, it is not just the information itself which can identify an individual. In the case of *Proceedings Commissioner v Commissioner of Police* [2000] NZAR 277, the Tribunal held that so long as information "had the capacity to identify [the individual] to some members of the public", it was personal information for the purposes of the Privacy Act.

The Act covers all New Zealand agencies unless a specific exception applies. An agency is defined as "*any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector; and, for the avoidance of doubt, includes a Department*".
Although this definition includes individuals as agencies, it does not include personal information relating to domestic affairs ("*individual's personal, family, or household affairs"*).

Any individual can make a complaint to the Privacy Commissioner and, following the Privacy (Cross-border Information) Amendment Act, any individual can make a subject access request to a New Zealand agency.

Exceptions are specific and laid down by law. The main exceptions from the scope of the Act are on political, constitutional and judicial grounds. The news media are exempt in relation to their news activities (similar to article 9 of the EU Directive).

Therefore the Working Party considers the scope of the application of the Privacy Act to be similar to that provided by the Directive.

3.2. Content principles

The Act contains twelve information privacy principles. These principles are not directly enforceable in a court of law apart from the right to access information held by a public sector agency. A complaint can be made to the Privacy Commissioner where there is an 'interference with privacy'. An 'interference with privacy' occurs where a breach of the principles is accompanied by harm or loss to the individual. With regards to the harm-based approach, the Privacy Commissioner confirmed that this is defined broadly in law and encompasses 'loss, detriment, damage or injury' through to 'adverse effect on rights, benefits, privileges, obligations'. Most importantly, the areas the Act explicitly provides for include emotional or mental harm in the form of 'significant humiliation, significant loss of dignity, significant injury to feelings'. For there to be an 'interference with privacy it is not necessary to show harm or loss in relation to subject access and correction principles.

Essential principles

> **1) The purpose limitation principle:** data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in article 13 of the Directive.

The Working Party considers that New Zealand implements this principle through its information privacy principles 1 (Purpose of collection of personal information), 10 (Limits on use of personal information), and 11 (Limits on disclosure of personal information).

Principle 1 provides that where an agency collects personal information, the purpose for its collection must be lawful; it must be connected with a function or activity of the agency; and it must be necessary for that purpose. Principles 10 and 11 require that the use or disclosure of personal information must conform to the purpose in connection with which it was obtained, or a directly related purpose.

Principle 10 provides for exceptions for secondary purposes. Principle 10(e) provides that an agency can use information for another purpose when it believes, on reasonable grounds, "*That the purpose for which the information is used is directly related to the purpose in connection with which the information was obtained*". Principle 11(a) also provides that an agency can disclose information to a person or body or agency when it believes, on reasonable grounds, *"That the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which the information was obtained*".

The secondary "*directly related purpose*" basis for using or disclosing personal information corresponds to the WP 12 requirement that personal data must be "*subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer"*.

Most of the other exceptions in principle 10 correspond to the exceptions under article 13 of the Directive. Those that do not reflect the provisions of article 7 of the Directive relating to legitimate purposes for processing. In addition, one exception provides for the Privacy Commissioner to authorise the processing. This is intended to cover unanticipated circumstances or those not covered by the Privacy Act. Details of these authorisations are in the Privacy Commissioner's annual report.

Therefore the Working Party considers that New Zealand legislation complies with this principle.

> **2) The data quality and proportionality principle:** Data should be accurate and, where necessary, kept up to date. The data should be appropriate, relevant and not excessive in relation to the purpose for which it is transferred or subsequently processed.

The Working Party considers that the data quality principle is implemented by information privacy principles 7 (Correction of personal information), 8 (Accuracy, etc, of personal information to be checked before use), and 9 (Agency not to keep personal information for longer than necessary). The proportionality principle is implemented by information privacy principle 1 (Purpose of collection of personal information).

Principle 8 provides that *"An agency that holds personal information shall 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 accurate, up to date, complete, relevant, and not misleading"*

Agencies have an obligation under principle 7(2) to correct information either on their own initiative or if requested by an individual so as to make sure the information is accurate, up to date, complete and not misleading. If an individual requests a correction that the agency is not willing to carry out, the individual can request that a statement of correction is attached to the existing information.

Retention is dealt with by principle 9 which provides that "*An agency that holds personal information shall not keep that information for longer than is required for the purposes for which*

the information may lawfully be used". The test of whether the information may lawfully be used is covered by principle 10 which limits the use of personal information.

Proportionality is covered by information privacy principle 1(a) which provides that information which is collected must be *"connected with a function or activity of the agency"*. Principle 1 (b) provides that the collection of the information must be *"necessary*" for the purpose for which it is being collected. There are Privacy Commissioner case notes and Human Rights Review Tribunal cases that have examined the interpretation of 'non-excessive' and the standard of necessity.

Therefore the Working Party considers that New Zealand legislation complies with this principle.

> **3) Principle of transparency:** Data subjects should be informed about the purpose for which the data are being processed and the identity of the processing controller in the third country, and any other aspect required to ensure fair treatment. The only exceptions allowed must be covered by articles 11(2) and 13 of the Directive.

The Working Party considers that transparency requirements are covered by information privacy principles 2 (Source of personal information), 3 (Collection of information from subject), and 4 (Manner of collection of personal information).

Principle 2(1) provides that "*Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.*" Principle 3(1) provides that "*when an agency collects personal information directly from the data subject, the agency must take reasonable steps in the circumstances to ensure that the data subject is aware of …"* and then lists the information to be provided to the individual. This list includes and goes beyond the elements of article 10 of the Directive.

The Privacy Act does not provide for notification of the individual when information is collected from a source other than the individual because, although there are some exceptions, the principle in the law is that information should not be collected from anyone other than the data subject. In any case the individual is protected by all of the other information privacy principles.

Principle 4 covers the issue of fairness by providing that an agency may not collect personal information:

(a) *By unlawful means; or*

(b) By means that, in the circumstances of the case, --

(i) Are unfair; or

(ii) Intrude to an unreasonable extent upon the personal affairs of the individual concerned.

Some of the exceptions to the transparency principle correspond to those in articles 11(2) and 13 of the Directive. However, some of the exceptions have no corresponding exception in the Directive. These are considered below.

(v) The agency believes, on reasonable grounds, that there is an authorization by data subject

The Act uses the term 'authorisation' rather than 'informed consent'. However, the Privacy Commissioner and the Tribunal have interpreted 'authorisation' to mean an active and deliberate form of signifying consent. One Privacy Commissioner case note stated that 'authorisation requires a positive act' and that a failure to object is not authorisation.

(vi) The agency believes, on reasonable grounds, that non-compliance would not prejudice data subject's interests
This exception comes from the harm-based approach adopted in New Zealand. It is similar in sprit to the balancing test required in article 7f of the Directive, although in New Zealand the test relates to the harm or loss that may be caused by the organisation's actions. To be cautious, organisations may well choose to notify the individual and get authorisation for the activity. This fits logically with the approach taken in New Zealand where the Act covers all personal information, including conversations, gossip and information in a person's mind. Under this framework, some flexibility is required to make the Act workable in practice and a harm-based approach is one way to achieve this. It is different from the European approach but nevertheless is unlikely to lead to any prejudice to the rights and freedoms of individuals. Personal information under this exception is still covered by the other information privacy principles.

(viii) The agency believes, on reasonable grounds, that compliance would prejudice the purposes of the collection
Although there is no exact corresponding exception in the Directive, this exception reflects the exceptions provided for in article 13(a) to (f) and is likely to be used in connection with monitoring and surveillance activities, in particular in the employment and law enforcement areas.

(xi) Special authority granted by Privacy Commissioner
This exception is intended to cover unanticipated circumstances not covered by the Act where processing personal data is desirable or necessary. The Commissioner will only issue an authorisation if she is satisfied that the public interest "*outweighs, to a substantial degree*", any possible potential harm to an individual as a result of the granting of the authorisation, or that authorisation would involve "a clear benefit to the individual concerned that outweighs" any possible potential harm that could result. The Privacy Commissioner may not grant an authorisation if the individual concerned has refused to authorise a collection, use, or disclosure of personal information. This means that the agency is first required to attempt to obtain the individual's consent. If the individual refuses to consent, the Commission cannot grant an authorisation.

Although the approach in New Zealand as regards transparency differs from the European approach in some areas, the Working Party is satisfied that the Act complies with this principle given that the basic rule under the Act is that personal information must always be collected directly from the individual concerned, with notification of purpose and other matters taking place at the time that the information is collected. Collecting information from other sources or not providing the required notification at the time of collection is treated as an exception to this basic rule.

> **4) Security principle:** The controller must adopt appropriate technical and organisational measures against the risks presented by the processing. Any person acting under the authority of the controller, including the person in charge of processing, must not process data except on instructions from the controller.

The Working Party considers that principle 5 (Storage and security of personal information) covers the aspects required for the security principle. This principle is based on the OECD security safeguards principle and the wording is similar to the wording of article 17(1) and (2) of the Directive in that security measures must protect against loss, access, use, modification, disclosure and misuse. Agencies must do everything reasonably within their power to prevent unauthorised access and disclosure where information is given to a processor. Processors using information beyond the controller's instructions would be in breach of several principles of the Act. Privacy Commissioner case notes show that particularly sensitive or private information (such as bank information) must be protected by stringent security safeguards. The principle is binding on both data controllers and data processors.

Therefore the Working Party considers that New Zealand law complies with the security principle.

> **5) Rights of access, rectification and opposition:** An individual must be entitled to a copy of all data relating to him or her, and the right to rectify any data that is inaccurate. In certain situations, the individual should also be able to oppose his or her data being processed. The only exceptions to these rights should be in line with Article 13 of the Directive.

The Working Party considers that the Act provides for rights of access and correction in principles 6 (Access to personal information) and 7 (Correction of personal information). Previously access and correction rights were restricted to individuals who were either a citizen or resident of, or physically in, New Zealand. However, the Privacy (Cross-border Information) Amendment Act 2010 amended the Privacy Act so that any individual can make *'information privacy requests'*. This includes: requests to obtain confirmation of whether or not an agency holds personal information; requests for access; and requests for correction. With regard to public sector agencies, the access right is a direct legal right and the individual can go straight to Court to enforce it rather than go through the Privacy Commissioner.

Most of the exceptions to the right of access are consistent with the provisions of article 13 of the Directive. The exception that covers national security and defence also covers international relations with other countries and international organisations, which is not specifically provided for in the Directive. However, the Working Party does not consider this to affect the level of adequacy.

There are a variety of exceptions that correspond to article 13(g), however, this section of the Act also includes exceptions related to administration that are not provided for in the Directive. These are considered below.

Access can be refused where "t*he request is frivolous or vexatious, or the information requested is trivial*." This is intended to prevent abuse of the access right and is similar to provisions found in European freedom of information legislation.

There are three practical administrative exceptions where information is "*not readily retrievable*", where it "*does not exist or cannot be found*", and where it is not held by the agency concerned, and there are no grounds for believing that it is held by another agency or that it is connected more closely with the functions or activities of another agency. In the latter case, the agency is obliged to transfer the access request to the relevant other agency.
As regards rights of opposition, there is no direct right under New Zealand law. However, under principle 3 (Collection of information from subject) individuals can object to processing at the time they are notified of it. Under principle 3(1)(e) and (f) individuals must be notified of the following.

> (e) *If the collection of the information is authorised or required by or under law,—*
> *(i) The particular law by or under which the collection of the information is so authorised or required; and*
> *(ii) Whether or not the supply of the information by that individual is voluntary or mandatory; and*
> *(f) The consequences (if any) for that individual if all or any part of the requested information is not provided.*

There are two reported cases where the Privacy Commissioner has investigated complaints where individuals were denied the opportunity to object. In one case relating to fishing regulations the agency changed its policy so only relevant questions were asked of the individual. In the other case

relating to club membership conditions, the club's constitution made clear what information was collected, the purposes of collection, and the recipients, so there was no breach of the principle.

WP 12 states that only in certain situations should individuals have a right of opposition, and that right exists for EU data in the EU before transfer to New Zealand. Therefore, the Working Party considers that New Zealand law complies with the principle of rights of access, rectification and opposition.

> **6) Restrictions on onward transfers to other countries:** Successive transfers of personal data from the third party destination country to another country may only be permitted if the latter also ensures an adequate level of protection. The only exceptions permitted should be those provided for in paragraph 1 of Article 26 of the Directive.

As New Zealand law is based on the OECD guidelines, there is no specific provision on protections and safeguards when personal data is transferred to a third country. Section 10 of the Act applies where New Zealand agencies hold information in a third country and this prevents agencies from avoiding the principles of the Act by being outside New Zealand. This provision also covers information held in a third country by a processor acting for a New Zealand agency. Principle 11 limits disclosures and this includes to agencies in third countries. The exceptions to this provision are largely consistent with the derogations in article 26 of the Directive. Even where information is in a third country, New Zealand agencies would still be responsible for any harm or loss arising from use or disclosure in that third country, and so it is in their interests to minimise the risk and ensure appropriate safeguards are in place.

The Privacy (Cross-Border Information) Amendment Act 2010 introduced provisions to refer cross-border complaints to the relevant authority and to empower the Privacy Commissioner in exceptional cases to prohibit the onward transfer of personal information received from overseas. The Privacy Commissioner has produced guidance to set out how the provision works and how her office intends to implement the new powers. The Commissioner can issue a transfer prohibition notice and breach of this notice would lead to criminal prosecution with the possibility of a $10,000 fine.

To serve a notice, the Commissioner must be satisfied that:

- the personal information has been received from another State and will be transferred to a third State where it will not be subject to a law providing comparable safeguards to the Privacy Act; and
- the transfer would be likely to breach the basic principles of national application set out in the OECD guidelines.

Before exercising the discretion to prohibit a transfer, the Commissioner must consider:

- the matters set out in section 114 (relating to human rights and other social interests that compete with privacy; international obligations on NZ; the information privacy principles; the public register privacy principles);
- whether or not the proposed transfer of personal information affects, or would be likely to affect, any individuals;
- the desirability of facilitating the free flow of information between NZ and other States; and
- any existing or developing international guidelines relevant to transborder data flows (including the OECD guidelines and the EU Directive).

With regard to effective cross-border enforcement, the provisions and the Commissioner's guidance mean that where European data protection authorities alert the Privacy Commissioner to a transfer,

the Commissioner will give priority to that case and be able to serve a prohibition notice if needed. The Commissioner also has investigative powers to proactively discover possible transfer arrangements that might warrant the exercise of the transfer prohibition powers.

The Working Party has some concerns as regards the effectiveness of the provisions in practice as it is not clear how the Commissioner will become aware of transfers out of New Zealand other than through data protection authorities. Nevertheless the changes in the law and the Commissioner's guidance have alerted businesses to the need to provide 'adequacy' in relation to any onward transfers on penalty of a transfer prohibition notice. In reality, given the geographical isolation of New Zealand from Europe, its size and the nature of its economy, it is unlikely that New Zealand agencies will have any business interest in sending significant volumes of EU-sourced data to third countries.

Although the Working Party does not consider that New Zealand law complies fully with the onward transfer principle, it does not believe that there is a major shortfall or that this needs to stand in the way of an 'adequacy' finding.

Additional principles
The WP12 document refers to certain principles that should be applied to specific types of processing, specifically the following.

> **1) Sensitive data:** In the case of "sensitive" data categories (those listed in Article 8 of the Directive), additional safeguards should be established, such as the requirement for individuals to give their explicit consent for data processing.

The Act does not distinguish between sensitive and non-sensitive data in the same way as the Directive; it regards all data as potentially sensitive and so subject to the same standards of protection. The categories of data set out in article 8 of the Directive are covered by provisions in the Human Rights Act 1993. As the data protection legislation in New Zealand predates the EU Directive, it has followed the approach set out in the OECD guidelines. In particular, this means the purpose-based approach, as the purpose for which information is collected will determine the circumstances for its use and disclosure under principles 10 and 11. In addition, Part 11 and Schedule 5 to the Privacy Act closely regulate access to law enforcement information by public sector agencies.

New Zealand has also followed the OECD guidelines by 'earmarking' certain categories of information as requiring particular attention. This is done through specific binding codes of practice. Health information is covered by the Health Information Privacy Code 1994, which contains more stringent provisions than the Act. Other codes are the Telecommunications Information Privacy Code 2003 and the Credit Reporting Privacy Code 2004. The Credit Reporting Code requires that credit reporters *"must not collect personal information for the purpose of credit reporting unless it is credit information"*.

Remedies for individuals are available under the Act if they suffer *"significant humiliation, loss of dignity, or injury to feelings"*. The emotional harm caused is judged on how the individual was actually affected by the breach, not how a hypothetical reasonable person would be affected.

As well as the provisions against discrimination contained in human rights law, other legislation provides protection for certain categories of data. For example, the Crimes Act 1961 deals with crimes against personal privacy and includes prohibitions on interception. The Private Investigators and Security Guards Act 1974 provides that private investigators may not take photographs or make visual recordings of a person without that person's prior written consent, and that such photographs

or recordings are not admissible in civil proceedings. Like some European countries, the freedom of information legislation contains provisions to prevent disclosure where this *"would involve the unwarranted disclosure of the affairs of another individual"* and there is no overriding public interest. There are also a number of cases where information has been found under the Privacy Act to have caused significant humiliation, loss of dignity, or injury to the feelings of individuals through their unauthorised collection, use or disclosure and these categories of data go beyond what is set out in article 8 of the Directive.

Therefore the Working Party considers that New Zealand law complies with the sensitive data principle.

> **2) Direct marketing:** Should the data transfer be for direct marketing purposes, the individual should be able to refuse to have his or her data used for this purpose at any time.

In considering this principle the Working Party accepts that New Zealand is a small country and direct marketing activities are not as developed as in other countries. There is no specific provision in the Act relating to direct marketing, however, the information privacy principles apply in the same way in this field. This includes the general principle that personal information, including that used for direct marketing, should be obtained directly from the individual. Thus circumstances in which personal information is transferred from the EU to New Zealand and used in New Zealand for direct marketing are likely to occur only rarely, if at all. Furthermore the Telecommunications Information Privacy Code 2003 limits the type of information that can be collected and its use. The code applies to network operators; telecommunications service providers; directory publishers and enquiry agencies, internet service providers, call centres that provide call centre services on contract to another agency, and mobile telephone retailers. The code only allows the use of telecommunications information for direct marketing with the individual's consent.

The Unsolicited Electronic Messages Act 2007 deals with spam and covers email, instant messaging, SMS and MMS of a commercial nature. It works in a similar way to Directive 2002/58/EC in that messages must only be sent to those who have given consent and must contain an unsubscribe facility.

The Commissioner has successfully dealt with many complaints about direct marketing.

In terms of self-regulation, the New Zealand Marketing Association and the Advertising Standards Authority have been proactive in educating members to protect the privacy of individuals. They have issued a code of practice and all marketers are expected to comply with its principles. There is a free complaints resolution service for individuals.

The New Zealand Marketing Association also operates free Do Not Mail and Do Not Call Services that cover unsolicited phone calls and mailings, although updated copies of the lists are only sent to its members.

Although the framework for dealing with direct marketing in New Zealand differs from that in Europe, in practice an individual has several ways to opt out. Even without a legal right to opt out, individuals can complain to the Privacy Commissioner, who has recognised that the law needs to be strengthened in this area. In reality, it is most unlikely that individuals in the EU will be sent direct marketing from New Zealand and so the Working Party considers that although New Zealand law does not comply fully with the direct marketing principle, it does not believe that there is a major shortfall or that this needs to stand in the way of an 'adequacy' finding.

3) Automatic individual decision: When the objective of a transfer is to take an automatic decision, in the sense of article 15 of the Directive, the interested party must have the right to know the reasoning behind this decision, and other measures must be taken to protect the person's legitimate interests.

The expert report makes clear that automated decision making is not common in New Zealand and there are various rules to discourage the practice. Some government information matching programmes allow some automated decision making, and these are regulated by Part 10 (Information matching) and Schedule 4 (Information matching rules) of the Privacy Act. The Commissioner has an oversight function for these programmes. The rules require safeguards for individuals which include checking the validity of automated results and providing information to individuals regarding any discrepancies and potential action against them.

The individual would normally need to be informed of the purpose for which personal information is being collected at the time of its collection (principle 3); the accuracy of personal information would need to be ensured before its use (principle 8); and personal information may not normally be used for any purpose other than that for which it was obtained (principle 10). Agencies making automated decisions also risk legal liability if their actions cause harm or loss to individuals.

With regard to the public sector, all individuals have a statutory right of access to the reasons for decisions affecting that person under the Official Information Act and the Local Government Official Information and Meetings Act. However, this only applies to New Zealand citizens and residents, or those physically in New Zealand.

Therefore, the Working Party considers that New Zealand law complies sufficiently with the automatic individual decision principle.

3.3. Procedural and enforcement mechanisms

WP 12 indicates that, to provide a basis for the assessment of the adequacy of the protection provided, it is necessary to identify the underlying objectives of a data protection procedural system, and on this basis to judge the range of different judicial and non-judicial procedural mechanisms used in third countries.

In this respect, the objectives of a data protection system are as follows.

– To deliver a good level of compliance with the rules.
– To provide support and help to individual data subjects in the exercise of their rights.
– To provide appropriate redress to the injured party where rules are not complied with.

a) To deliver a good level of compliance with the rules: a good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them.
The existence of effective and dissuasive sanctions can play an important part in ensuring respect for the rules, as can systems of direct verification by authorities, auditors, or independent data protection officials.

Awareness among data controllers and individuals

The Privacy Act has been in force since 1993 and requires every public and private sector agency to have at least one privacy officer. They are responsible for encouraging their agency's compliance with the information privacy principles; dealing with access requests; working with the Privacy Commissioner in case of an investigation; and otherwise ensuring their agency's compliance with the Privacy Act. There are several privacy officer networks around the country that hold meetings.

The Office of the Privacy Commissioner has extensive information on its website and publishes a quarterly newsletter, as well as anonymised case notes on selected investigations. The Office carries out regular training sessions and workshops around the country for privacy officers and others and is involved in the annual Asia-Pacific Privacy Awareness week. The Office carries out surveys every few years to measure awareness as well as the effectiveness of the Commissioner.

The Office of the Privacy Commissioner

The Privacy Commissioner is a Crown entity that is required to act independently in relation to the functions, duties, and powers of the office. The Privacy Commissioner is appointed by the Governor-General (the representative of the Head of State in New Zealand) on the recommendation of the responsible Minister - the Minister of Justice. Appointment by the Governor-General is a special high-level procedure reserved for a small number of important statutory appointments. To recommend a person for appointment as Commissioner, the responsible Minister must be of the opinion that the person has the appropriate knowledge, skills, and experience to assist the statutory entity to achieve its objectives and perform its functions. Section 13(1A) of the Privacy Act provides that the Commissioner must act independently in performing his or her statutory functions and duties and in exercising his or her statutory powers.

The Office of the Privacy Commissioner is required to report annually to Parliament. These reports include details of all the authorised information matching programmes carried out during the year and an assessment of their compliance.

The Privacy Commissioner functions as an ombudsman, investigating and attempting to conciliate complaints, carrying out own-motion investigations. She also has functions set out in the Act, such as education, monitoring compliance, giving policy advice, responding to inquiries, reporting to the Prime Minister, and so on. Part 9 of the Act gives the Privacy Commissioner powers to do such things as summon and examine witnesses on oath, and require them to provide information and documents within 20 working days.

The Commissioner also has powers, functions and duties under legislation other than the Privacy Act (such as under the Health Act, the Social Security Act, the Domestic Violence Act, and the Passports Act).

In addition the Office of the Privacy Commissioner has been accredited to the International Conference of Data Protection and Privacy Commissioners; has been approved as a participant of the APEC Cross-border Privacy Enforcement Arrangement; and has been recognised to participate as a member of the Global Privacy Enforcement Network.

Enforcement means and sanctions

Part 9 of the Act (Proceedings of Commissioner) sets out the investigation procedure and powers of the Privacy Commissioner. It is an offence to fail to co-operate or interfere with the Privacy Commissioner's investigations, with a fine of up to $2,000.

If a complaint cannot be resolved by the Commissioner, it may be referred to the Human Rights Review Tribunal if the complainant or the Director of Human Rights Proceedings decides to pursue the matter further. A complainant can ask the Director to refer the case to the Tribunal even if the Privacy Commissioner declines to do so. A full range of remedies is available in the Tribunal, including compensatory damages and orders in the nature of prohibitory and mandatory injunctions. The media tend to report such decisions and the small size of New Zealand means that negative publicity has a dissuasive effect. Where the Director of Human Rights Proceedings has decided not

to represent a complainant the Privacy Commissioner is normally represented in proceedings where, as is often the case, the complainant is not represented by legal counsel, and there is an important legal principle at issue under the Privacy Act. The Privacy Commissioner's right to appear or be represented in these cases provides that she can appear and be heard in any proceedings in which the Director of Human Rights Proceedings would be entitled to appear and be heard, but declines to do so. The Director of Human Rights Proceedings also has the power to bring a class action on behalf of several individuals, although this has not yet happened.

As mentioned earlier, the Privacy (Cross-Border Information) Amendment Act 2010 gives the Commissioner the power to issue transfer prohibition notices in relation to transfers from New Zealand to third countries without an adequate level of protection.

In the light of all this, the Working Party believes that the New Zealand legislation has put in place the necessary elements to deliver a good level of compliance with the rules on data protection.

> **b)** To provide **support and help to individual data subjects** in the exercise of their rights. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. In order to do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

As previously mentioned the Privacy Commissioner is required to act independently in relation to the functions, duties, and powers of the office. The Office has put mechanisms in place over the last few years to deal more effectively with complaints and reduce backlogs. The Privacy Commissioner has the power to summon parties to compulsory conferences to deal with a complaint, with the aim of identifying the relevant matters and trying to get agreement between the parties on the resolution. Sometimes the Office may arrange independent or in-house mediation to resolve disputes. Agencies may make agreed settlements which can provide remedies that are not specifically provided for under the Privacy Act.

There is no charge for individuals in taking complaints to the Commissioner or in being represented by the Director of Human Rights Proceedings in court. Complainants can take cases to to the Human Rights Review Tribunal themselves and there are no costs for filing the case and no requirement to be represented by a lawyer. However, if the complainant loses the case, they may be liable for a contribution to the actual and reasonable legal costs of the successful party.

The Working Party considers that New Zealand legislation offers sufficient mechanisms to provide assistance and support to individuals.

> **c)** To provide **appropriate redress** to the injured party where rules are not complied with. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

Most privacy complaints are either resolved by the Commissioner or not proceeded with after investigation. The numbers of cases taken to the Human Rights Review Tribunal is fairly constant at approximately 20 a year.

The Tribunal has the power to issue declarations, restraining orders, and to suppress details about a case or hold part or all of the hearing in private. The Tribunal can also award compensatory damages up to a maximum of $200,000; the highest amount to date under the Privacy Act was $40,000 awarded for *"humiliation, loss of dignity, and injury to the feelings of the aggrieved*

individual". Where the amount claimed in damages is over $200,000, the Tribunal can refer a matter to the High Court to award the damages.

The Tribunal can make orders to specify action required by the agency, such as disclosing information where an access request was denied. It can also make orders for "*other relief*" to cover remedies not provided for under the Act.

Tribunal decisions can be appealed to the High Court if they concern a question of fact, and High Court decisions can be appealed to the Court of Appeal on a question of law only. If the High Court refuses leave to appeal, the Court of Appeal can grant this if it believes that the point of law is important enough for it to debate. The same process applies for appeals to the Supreme Court.

Therefore the Working Party considers that New Zealand law provides appropriate redress.

4. Result of the assessment

New Zealand data protection and privacy law largely predates the EU Directive and implements the OECD guidelines. There have though been some recent amendments specifically to address concerns about 'adequacy' for transfers of personal data from the EU. The Working Party recalls that although some concerns still exist, adequacy does not mean equivalence with the Directive.

Therefore the Working Party considers that **New Zealand ensures an adequate level of protection** within the meaning of Article 25(6) of Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.

However, the Working Party also encourages the New Zealand authorities to take the necessary steps to address weaknesses in the current legal framework. In particular, the Working Party encourages the Privacy Commissioner to continue her call for strengthening the law in relation to direct marketing; and to maintain effective oversight of transfers from New Zealand to third countries which are not themselves subject to an adequacy finding. The Working Party also requests that, in addition to considering OECD guidelines and the EU Directive, the Privacy Commissioner also considers relevant European Commission decisions and Article 29 Working Party guidance when deciding whether to issue a transfer prohibition notice.

The Working Party also highlights the fact that, as part of any decision taken by the Commission, it will closely follow the evolution of data protection in New Zealand and the way in which the Office of the Privacy Commissioner applies the principles of data protection referred to in document WP12 and in this document.

Done at Brussels, on 4 April 2011

For the Working Party
The Chairman
Jacob KOHNSTAMM