Periodic Update Report

On Developments in Data Protection Law

In New Zealand

(2013-2015)

_____

Report to the European Commission

by the competent supervisory authority

for the application of the legal data protection standards

in New Zealand

December 2015

_____

Privacy Commissioner
Te Mana Matapono Matatapu
New Zealand

Table of contents

Letter of Introduction

Bruno Gencarelli
Head of Unit – Data Protection European Commission
Directorate-General for Justice
Brussels
Belgium

Dear Bruno

Periodic update report on developments on data protection law in New Zealand

I am pleased to take this opportunity to update the European Commission in relation to the legal standards for the protection of personal data in New Zealand.

This is the first formal written report submitted since the European Commission issued its decision in late 2012 recognising New Zealand's legal standards as being sufficient for Article 25(2) of European Union Directive 95/46/EC.

While this is the first report, my office has of course corresponded over that period with the Commission and both I and my staff have met with you. At our most recent meeting we agreed that brief written reports might be of assistance to assist the EC's ongoing monitoring of the New Zealand decision as a 'living document'.

The fundamentals of New Zealand law which established our case to be considered as ensuring an adequate level of protection for personal data remain in place. There have been several developments over the last three years that touch upon existing legal protections and, in some cases, raise standards and provide additional legal protections.

The report only briefly canvasses selected developments. My office remains available to answer questions if more details are needed on the matters mentioned or any other areas of interest to the EC.

Yours sincerely

John Edwards
New Zealand Privacy Commissioner

1. Background

1.1 On 19 December 2012 The European Commission formally decided that for the purposes of Article 25(2) of the Directive 95/46/EC (the EU Data Protection Directive), New Zealand is considered as ensuring an adequate level of protection for personal data transferred from the European Union. The text of the EC decision is annexed to this report.

1.2 The decision records that the competent supervisory authority for the application of the legal data protection standards in New Zealand is the Privacy Commissioner.

1.3 Article 4 of the EC decision records that the Commission must monitor the functioning of the decision. The competent supervisory authority has periodically corresponded and met with EC staff to assist the EC to perform its monitoring task. At the most recent meeting in October 2015, the Privacy Commissioner offered, and the EC staff accepted, to commence periodically submitting update reports to facilitate monitoring. It is anticipated that such reports will be provided at 6 monthly intervals and focus, in particular, on any relevant changes to New Zealand's Privacy Act. The reports may also record other developments of importance bearing upon the level of protection of personal data New Zealand.

1.4 This first report under this new arrangement will briefly survey developments since the commencement of the EC decision in 2013.

1.5 The report is being submitted in the Privacy Commissioner's capacity as the independent supervisory authority with competence under Article 1(2) of the decision. It is understood by the EC that the Privacy Commissioner does not purport to speak for the New Zealand Government

2. Statutory amendments to New Zealand privacy law

2.1 The legal standards for the protection of personal data in New Zealand are primarily set out in the Privacy Act 1993. It covers the entire public and private sectors, with a few specific public interest exceptions that one would expect in a democratic society.

2.2 As with any other piece of legislation, the Privacy Act is frequently amended in minor technical ways (for example, changing statutory cross-references) or by giving effect to matters of detail within the normal scheme of the Privacy Act (for example, by listing additional authorised information matching programmes). However, substantive amendments to the Privacy Act are relatively rare. During the three year period there were only two noteworthy sets of amendments. These were made respectively by the:

- Privacy Amendment Act 2013.
- Harmful Digital Communications Act 2015. (In addition to amending the Privacy Act, this Act created new redress for cyber bullying - see Part 3 of this report.)

2.3 The Privacy Amendment Act 2013 amended the Privacy Act in two substantive ways:

- By widening the exceptions to Information Privacy Principles 10 and 11 as they relate to serious threats to public health, public safety or health of individuals.
- By inserting a new Part 9A into the Privacy Act creating a new regulatory regime as an option to enable the sharing of personal information to facilitate the provision of public services.

2.4 *Serious threats*: It is quite usual to have an exception to data protection controls to enable disclosure of personal information to respond to serious threats to individuals or the public at large. The Law Commission, which is responsible for systematic law reform in New Zealand, reviewed the wording of the provision and recommended that the law be redrafted to make it clearer and more effective. In particular, it recommended that a requirement that a serious threat be 'imminent' before the exception was available be omitted to allow for more rapid use or disclosure of information if necessary to respond to a serious threat. The government accepted this advice and the Parliament duly amended the law in the manner recommended by the Law Commission. The main change was effected by including a new definition in the Act of 'serious threat' which is referenced in the use and disclosure principles. The definition sets out a test recommended by the Law Commission:

'**serious threat**, for the purposes of principle 10(d) or 11(f), means a threat that an agency reasonably believes to be a serious threat having regard to all of the following:
(a) the likelihood of the threat being released; and
(b) the severity of the consequences if the threat is realised: and
(c) the time at which the threat be may realised.'

2.5 *New Part 9A Information Sharing*: The 2013 amendment inserted Part 9A into the Act. Section 96A explains the purpose of the Part which is 'to enable the sharing of personal information to facilitate the provision of public services'. To achieve that purpose, the Part provides a mechanism for the approval of 'information sharing agreements' for the sharing of information between or within agencies, authorises exemptions from or modifications to information privacy principles or codes of practice, and reduces uncertainty about whether personal information can lawfully be shared for the provision of public services in the circumstances described in the approved information sharing agreement.

2.6 The detailed provisions of Part 9A address questions of authority, scope, approval processes, reporting requirements, notification requirements, responsibilities of parties and review of agreements. The processes require consultation with the Privacy Commissioner who is given a special reporting function. The legislative instrument approving an authorised information sharing agreement must be presented to Parliament and is subject to disallowance by resolution of House of Representatives. As with all delegated legislation, the legislative instrument is routinely examined by Parliaments Regulations Review Committee which can initiate disallowance if the instrument trespasses unduly on personal rights and liberties.

2.7 The Act has been amended to ensure that complaints can be taken, and redress is available, in relation to alleged non-compliance with an authorised information sharing agreement.

2.8 Since coming into force in 2013, three authorised information sharing agreements have been issued:

- *Privacy (Information Sharing Agreement between Inland Revenue and New Zealand Police) Order 2014* – to enable certain tax information to be shared with the Police for the purpose of the prevention, detection, or investigation of a serious crime, or as evidence of a serious crime, or, in anonymised form, for producing police data on crime trends.

- *Privacy (Information Sharing Agreement between Inland Revenue and Internal Affairs) Order 2014* (replacing a 2013 order) - to supply Inland Revenue with passport information relating to overseas-based borrowers and liable parents living overseas who are in default of their student loan repayment or child support payment obligations or have not kept their contact details with Inland Revenue up to date.
- *Privacy (Information Sharing Agreement for Improving Public Services for Vulnerable Children) Order 2015* – to enable a group of designated agencies, under the lead of the Ministry of Social Development, to share information to facilitate co-ordinated and collaborative action across agencies to better identify, support, and protect vulnerable children.

2.9 The Harmful Digital Communications Act 2015 amended the Privacy Act in two substantive ways:

- By modifying the exceptions to the use and disclosure principles in relation to information sourced from a publicly available publication;
- By limiting the circumstances in which the domestic affairs exemption is available.

2.10 *Publicly available publication exceptions*: The information privacy principles in the Privacy Act governing the use and disclosure of personal information each contain an exception permitting use or disclosure where 'the source of the information is a publicly available publication'. The Harmful Digital Communications Act added a caveat to each exception to provide the words 'and that, in the circumstances of the case, it would not be unfair or unreasonable to use the information.'

2.11 The amendments to the principles narrow the exceptions and therefore can be said to have raised the standard of protection of personal information. The additional words were added on the recommendation of the Law Commission and arose out of work to identify gaps in the statutory protections for individuals in the online environment.

2.12 *Domestic affairs exemption:* as is common in many privacy laws, the Privacy Act contains an exception relating to the collection and use of personal information held by individuals solely or principally for the purposes of, or in connection with, the individual's personal, family or household affairs. The amendment made by the Harmful Digital Communications Act added

a caveat limiting the availability of that exemption in certain cases. A new sub-section was inserted that provided that the exemption:

> 'ceases to apply once the personal information concerned is collected, disclosed, or used if that collection, disclosure or use would be highly offensive to an ordinary reasonable person.'

2.13 The narrowing of the domestic affairs exemption might be characterised as increasing the standard of legal protection to personal information in New Zealand. The change was made on the recommendation of the Law Commission which is responsible for systematic law reform in New Zealand.

3. Other statutory developments

3.1 While the legal standards for the protection of personal data in New Zealand are primarily set out in the Privacy Act, there are a number of regulatory frameworks for dealing with privacy issues in terms of policy, rules or complaints jurisdictions.

3.2 The only new enactment of significance during the three year period covered by this report is the Harmful Digital Communications Act 2015.

3.3 The Harmful Digital Communications Act states its purpose to be to:

- deter, prevent and mitigate harm caused to individuals by digital communications; and
- provide victims of harmful digital communications with a quick and efficient means of redress.

3.4 The Act was developed by the Law Commission as part of its study of gaps in the legal protections available to New Zealand for harms caused by online behaviour. The Law Commission considered a variety of harms such as 'cyber-bullying' and harassment. Although not the principal focus, privacy harms naturally emerged from its study.

3.5 The Harmful Digital Communications Act is built around 10 'communications principles'. While many of these principles have no direct relevance to the level of protection of personal data in New Zealand, several are relevant including:

- Principle 1: A digital communication should not disclose sensitive personal facts about an individual.
- Principle 7: A digital communication should not contain a matter that is published in breach of confidence.

3.6 Several of the other principles although not directly framed around protection of personal information, nonetheless are focused upon preventing harm to individuals or enabling redress when harm has occurred and these can have some direct relevance to privacy cases. For example:

- Principle 2: A digital communication should not be threatening, intimidating, or menacing.
- Principle 5: A digital communication should not be used to harass an individual.
- Principle 8: A digital communication should not incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual.
- Principle 9: A digital communication should not incite or encourage an individual to commit suicide.

3.7 The Act provides a process for better giving effect to such principles. For example, it establishes a role for an 'approved agency' which will take account of the communications principles in performing functions under the Act. Once established, complaints will be able to be taken to the approved agency which will focus upon attaining speedy and practical solutions for harmed individuals by, for example, encouraging the taking down of harmful content that has been posted on line. There is also provision for proceedings to be brought in the District Court.

4. Other developments

4.1 In an area law as dynamic as data protection, there are always developments of interest. To keep this report to a reasonable length, only one area of interest will be touched upon developments of relevance to the protection of personal data as it relates to intelligence organisations. I am aware that this is a matter that has been of interested to the European Parliament and to the EC.

4.2 The Privacy Act defines 'intelligence organisation' to mean:

- the New Zealand Security Intelligence Service; and
- the Government Communications Security Bureau.

4.3 There is a partial exemption from the information privacy principles for intelligence organisations and for information disclosed to intelligence organisations. The Act provides that 'Nothing in principles 1 – 5 or principles 8- 11 applies in relation to information collected, obtained, held, used, or disclosed by, or disclosed to, an intelligence organisations.'

4.4 On the basis of that exemption, it can be seen that principle 6 and 7 (subject access and correction) and 12 (unique identifiers) apply to intelligence organisations. Accordingly, individuals are entitled by law to ask intelligence organisations if information is held about them and to seek access. If denied access, they are entitled to take a complaint to the Privacy Commissioner. Similarly, whether or not given access, they can pursuant to law ask intelligence organisations to correct information held about them. A refusal to correct information may also be taken by complaint to the Privacy Commissioner.

4.5 The Act provides special procedures for complaints against intelligence organisations. The principal difference in the procedure from ordinary complaints is that proceedings may not be taken to the Human Rights Review Tribunal either by the Commissioner or the aggrieved individual. In the event that the Commissioner upholds a complaint that cannot be resolved, a special procedure exists for the Privacy Commissioner to report to the Prime Minister.

4.6 A noteworthy legislative development during the period was the enactment of the Government Communications Security Bureau Amendment Act 2013. Amongst other things,

the Amendment inserted new sections 25A and 25B into the Act governing the Government Communications Security Bureau. These provide:

> **25A Formulation of policy on personal information**
> (1) As soon as is reasonably practicable after the commencement of this section, the Director must, in consultation with the Inspector-General of Intelligence and Security and the Privacy Commissioner, formulate a policy that applies to the Bureau (in a manner compatible with the requirements of national security) the principles set out in section 25B.
> (2) The policy must require—
> (a) all employees and persons acting on behalf of the Bureau to comply with the policy; and
> (b) the level of compliance with the policy to be regularly audited.
> (3) The Director must advise the Privacy Commissioner of the results of audits conducted under the policy.
> (4) The Privacy Commissioner may provide a report to the Inspector-General of Intelligence and Security if the results of the audits disclose issues that need to be addressed.
> (5) The Director must regularly review the policy at intervals of not more than 3 years and, if he or she considers it appropriate to do so, revise the policy in consultation with the Inspector-General of Intelligence and Security and the Privacy Commissioner.
>
> **25B Principles to protect personal information**
> The principles referred to in section 25A(1) are as follows:
> (a) the Bureau must not collect personal information unless—
> (i) the information is collected for a lawful purpose connected with a function of the Bureau; and
> (ii) the collection of the information is reasonably necessary for that purpose, having regard to the nature of intelligence gathering:
> (b) the Bureau must ensure—
> (i) that any personal information it holds is protected by such security safeguards as it is reasonable in the circumstances to take against—
> (A) loss; and
> (B) access, use, modification, or disclosure, except with the authority of the Bureau; and
> (C) other misuse; and
> (ii) that if it is necessary for any personal information that it holds to be given to a person in connection with the provision of a service to the Bureau, everything reasonably within the power of the Bureau is done to prevent unauthorised use or unauthorised disclosure of the information:
> (c) the Bureau must not use personal information without taking such steps (if any) as are, in the light of the interests and constraints of national security and the nature of intelligence gathering, 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:
> (d) the Bureau must not keep personal information longer than is required for the purposes for which the information may be lawfully used.

4.7 The principles referred to in section 25B are modelled upon several of the information privacy principles in the Privacy Act that are not directly applied to the intelligence organisations, namely, information privacy principles 1, 5, 8 and 9. The GCSB has commenced work to formulate the required policies on personal information.

5. Further information and reports

5.1 Further information about any aspect of this report may be requested from Blair Stewart, Assistant Commissioner (Auckland), Office of the Privacy Commissioner at blair.stewart@privacy.org.nz.

5.2 It is intended that future reports be provided at approximately six monthly intervals. As this is the first such report, the Office of the Privacy Commissioner welcomes feedback as to its usefulness. In the absence of any particular feedback, it will be intended that this format be followed each time. Future reports will likely be considerably shorter than this report given the extended period this first report covers.

5.3 It is anticipated that future reports might be provided in June and December or thereabouts.

Annex: European Commission Decision of 19 December 2012

COMMISSION IMPLEMENTING DECISION

of 19 December 2012

pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand

(notified under document C(2012) 9557)

(Text with EEA relevance)

(2013/65/EU)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

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 Article 25(6) thereof,

After consulting the European Data Protection Supervisor

Whereas:

(1)Pursuant to Directive 95/46/EC, Member States are required to provide that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection and if the Member States' laws implementing other provisions of the Directive are complied with prior to the transfer.

(2)The Commission may find that a third country ensures an adequate level of protection. In that case, personal data may be transferred from the Member States without additional guarantees being necessary.

(3)Pursuant to Directive 95/46/EC the level of data protection should be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations and giving particular consideration to certain specified elements relevant for the transfer.

(4)Given the different approaches to data protection in third countries, the adequacy assessment should be carried out, and any decision based on Directive 95/46/EC should be made and enforced in a way that does not arbitrarily or unjustifiably discriminate against or between third countries where like conditions prevail, nor constitute a disguised barrier to trade, regard being had to the Union's present international commitments.

(5)New Zealand is a former British colony. It became an independent Dominion in 1907, but did not formally sever its constitutional ties with Great Britain until 1947. New Zealand is a unitary State and does not have a written constitution in the conventional sense of an entrenched constitutive

document. The country is a constitutional monarchy and parliamentary democracy on the Westminster model, with the Queen of New Zealand as the Head of State.

(6)New Zealand operates on the principle of Parliamentary sovereignty. Nevertheless, by convention there are a number of statutes that are of particular constitutional importance and are regarded as 'higher law'. This is in the sense that they form part of the constitutional background or landscape by informing government practice and the enactment of other legislation. Moreover, cross-political consensus would be expected in the event of amendment or repeal of this legislation. Several of these statutes — the Bill of Rights Act of 28 August 1990 (Public Act No 109 of 1990), the Human Rights Act of 10 August 1993 (Public Act No 82 of 1993), and the Privacy Act of 17 May 1993 (Public Act No 28 of 1993) — are relevant to data protection. The constitutional importance of this legislation is reflected by the convention that they must be taken into account when developing or proposing new legislation.

(7)The legal standards for the protection of personal data in New Zealand are primarily set out in the Privacy Act, as amended by the Privacy (Cross-border Information) Amendment Act of 7 September 2010 (Public Act No 113 of 2010). It predates Directive 95/46/EC, and is not limited to automatically processed data or structured data in a filing system, but covers all personal information in whatever shape or form. It covers the entire public and private sectors, with a few specific public interest exceptions that one would expect in a democratic society.

(8)There are a number of regulatory frameworks in New Zealand for dealing with privacy issues in terms of policy, rules, or complaints jurisdictions. Some are statutory while others are self-regulating industry bodies, including media regulation, direct marketing, unsolicited electronic messages, market research, health and disability, banking and insurance and savings.

(9)In addition to legislation enacted by the New Zealand Parliament, there exists a considerable body of common law whose roots stem from English common law, embodying common law principles and rules that are relevant to data protection. Among the fundamental common law principles is the principle that the dignity of the individual is a paramount concern of the law. This common law principle is a key element in the background context to judicial decision-making generally in New Zealand. New Zealand case-law based on common law also contains a number of other aspects of privacy including invasion of privacy, breach of confidence and incidental protection in the context of defamation, nuisance, harassment, malicious falsehood, negligence and others.

(10)The legal data protection standards applicable in New Zealand cover all the basic principles necessary for an adequate level of protection for natural persons, and also provide for exceptions and limitations in order to safeguard important public interests. These legal data protection standards and the exceptions reflect the principles laid down in Directive 95/46/EC.

(11)The application of the legal data protection standards is guaranteed by administrative and judicial remedies, and by independent supervision carried out by the supervisory authority, the Privacy Commissioner, who is endowed with the kinds of powers set out in Article 28 of Directive 95/46/EC, and who acts independently. Moreover, any interested party is entitled to seek judicial redress for compensation for damages suffered as a result of the unlawful processing of his personal data.

(12)New Zealand should therefore be regarded as providing an adequate level of protection for personal data as referred to in Directive 95/46/EC.

(13)This decision should concern the adequacy of protection provided in New Zealand with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC. It should not affect other conditions or restrictions implementing other provisions of the Directive that pertain to the processing of personal data within Member States.

(14)In the interest of transparency and in order to safeguard the ability of the competent authorities in the Member States to ensure the protection of individuals as regards the processing of their personal data, it is necessary to specify the exceptional circumstances in which the suspension of specific data flows may be justified, notwithstanding the finding of adequate protection.

(15)The Working Party on the protection of individuals with regard to the processing of personal data established under Article 29 of Directive 95/46/EC has delivered a favourable opinion on the level of adequacy as regards protection of personal data in New Zealand, which has been taken into account in the preparation of this Implementing Decision.

(16)The measures provided for in this Decision are in accordance with the opinion of the Committee established under Article 31(1) of Directive 95/46/EC,

HAS ADOPTED THIS DECISION:

Article 1

1. For the purposes of Article 25(2) of Directive 95/46/EC, New Zealand is considered as ensuring an adequate level of protection for personal data transferred from the Union.

2. The competent supervisory authority for the application of the legal data protection standards in New Zealand is set out in the Annex to this Decision.

Article 2

1. Without prejudice to their powers to take action to ensure compliance with national provisions adopted pursuant to provisions other than Article 25 of Directive 95/46/EC, the competent authorities in Member States may exercise their existing powers to suspend data flows to a recipient in New Zealand in order to protect individuals with regard to the processing of their personal data in the following cases:

(a)where a competent New Zealand authority has determined that the recipient is in breach of the applicable standards of protection; or

(b)where there is a substantial likelihood that the standards of protection are being infringed, there are reasonable grounds for believing that the competent New Zealand authority is not taking or will not take adequate and timely steps to settle the case at issue, the continuing transfer would create an imminent risk of grave harm to data subjects and the competent authorities in the Member State have made reasonable efforts in the circumstances to provide the party responsible for processing established in New Zealand with notice and an opportunity to respond.

2. The suspension shall cease as soon as the standards of protection are assured and the competent authority of the Member States concerned is notified thereof.

Article 3

1. Member States shall inform the Commission without delay when measures are adopted on the basis of Article 2.

2. The Member States and the Commission shall inform each other of cases where the action of bodies responsible for ensuring compliance with the standards of protection in New Zealand fails to ensure such compliance.

3. Where information gathered under Article 2(1) and under paragraphs 1 and 2 of this Article provides evidence that any body responsible for ensuring compliance with the standards of protection in New Zealand is not effectively fulfilling its role, the Commission shall inform the competent New Zealand authority and, if necessary, present draft measures in accordance with the procedure referred to in Article 31(2) of Directive 95/46/EC with a view to repealing or suspending this Decision or limiting its scope.

Article 4

The Commission shall monitor the functioning of this Decision and report any pertinent findings to the Committee established under Article 31 of Directive 95/46/EC, including any evidence that could affect the finding in Article 1 of this Decision, that protection in New Zealand is adequate within the meaning of Article 25 of Directive 95/46/EC and any evidence that this Decision is being implemented in a discriminatory manner.

Article 5

Member States shall take all the measures necessary to comply with this Decision until 20 March 2013.

Article 6

This Decision is addressed to the Member States.

Done at Brussels, 19 December 2012.

For the Commission

Viviane REDING

Vice-President

ANNEX

Competent supervisory authority referred to in Article 1(2) of this Decision:

Privacy Commissioner:
Te Mana Matapono Matatapu
Level 4
109-111 Featherston Street
Wellington 6143
New Zealand
Tel: +64-4-474 7590
Contact e-mail: enquiries@privacy.org.nz
Website: http://privacy.org.nz/