Periodic Update Report
On
Developments in Data Protection Law
In New Zealand

(January – June 2017)

_____

Fifth Report to the European Commission

By the Competent Supervisory Authority

For the Application of the Legal Data Protection Standards

In New Zealand

26 June 2017

_____

Privacy Commissioner
Te Mana Matapono Matatapu
New Zealand

Table of Contents

13 June 2017

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

Dear Bruno

Update report on developments in New Zealand data protection law

I submit this 5th report to update the European Commission in relation to matters bearing upon the legal standards for the protection of personal data in New Zealand for the 6 months since my last report dated 9 December 2016.

I am pleased to be able to report that during the period there was an amendment to the law concerning the activities of intelligence and security agencies that may be characterised as strengthening the legal standards for the protection of personal data in New Zealand.

Yours sincerely

John Edwards
New Zealand Privacy Commissioner

1. Background

On 19 December 2012 the European Commission formally decided that 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 EU.

The EC has a responsibility to monitor the functioning of the decision. To assist the EC to undertake this monitoring, the New Zealand Privacy Commissioner as 'the competent supervisory authority for the application of the legal data protection standards in New Zealand' has undertaken periodically to submit update reports on developments in New Zealand data protection law.

On 22 December 2015 the Privacy Commissioner submitted the first report that briefly surveyed developments since the commencement of the EC decision in 2013. That initial report was updated by other reports dated 2 March (supplement), 30 June and 9 December 2016. This report covers the period January to June 2017 (inclusive).

Regulation (EU) 2016/679 of 27 April 2016 (known as the General Data Protection Regulation or GDPR) will repeal Directive 95/46/EC when it comes into effect next year on 25 May 2018. However, Article 45(9) of the GDPR provides that the decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC will remain in force until amended, replaced or repealed by a Commission decision adopted in accordance with Article 45(3) or (5) of the new regulation. Accordingly, the EC adequacy decision covering New Zealand will continues in the new GDPR regime.

In this report the Privacy Commissioner does not purport to speak for the New Zealand Government.

2. Statutory amendments to New Zealand privacy law

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

Privacy Act amended by Intelligence and Security Act 2017

One such exemption relates to the activities of intelligence organisations (i.e. the New Zealand Security Intelligence Service and the Government Communications Security Bureau). The Privacy Act was amended in 2017 to narrow the partial exemption as it related to these organisations and to replace the complete exemption for disclosures by other agencies to those organisations with a specific exception to the disclosure principle. The amendment will not come into force until September this year.

Existing law
Since its inception in 1993 the Privacy Act has:

- Provided the intelligence organisations with a partial exemption from 8 of the 12 information privacy principles (section 57); and
- Completely exempted from information privacy principle 11 any disclosures that are made by any agency to intelligence organisations (section 57).

Changes made by Intelligence and Security Act 2017

The 2017 Act has narrowed the partial exemption enjoyed by the intelligence organisations (now renamed intelligence and security agencies) so that they are now exempt from only 3 of the 12 information privacy principles rather than from 8 as formerly. This can be shown as follows:

Narrowing of partial exemption for intelligence organisations/agencies	
Existing Act (section 57)	**Amended Act** (section 57)
Intelligence organisations *Nothing in principles 1 to 5 or principles 8 to 11 applies in relation to information collected, obtained, held, used, or disclosed by, or disclosed to, an intelligence organisation.*	**Exemption for intelligence and security agencies** *Information privacy principles 2, 3, and 4(b) do not apply to information collected by an intelligence and security agency.*

The application of the additional principles imposes new statutory duties on the intelligence agencies and corresponding accountabilities such as the right for individual complaint.

The information privacy principles governing the use and disclosure of personal information contain a list of specific exceptions where use and disclosure is permitted. Exceptions have been inserted into two principles to provide the permitted scope of use and disclosure by intelligence and security agencies. This can be shown as follows:

	Existing Act (section 57) Complete exemption	**Amended Act (section 57) Exceptions stated in principle (section 6)**
Use	*Nothing in … principles 8 to 11 applies in relation to information … used … by… an intelligence organisation.*	New principle 10(2): *In addition to subclause (1), an intelligence and security agency that holds personal information that was obtained in connection with one purpose may use the information for any other purpose (a secondary purpose) if the agency believes on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions.*
Disclosure	*Nothing in … principles 8 to 11 applies in relation to information … disclosed by … an intelligence organisation.*	New principle 11(fa) authorises disclosure by an agency that believes on reasonable grounds that *the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions*

There are no exceptions inserted into the other principles newly applied to the intelligence organisations including principles 1 (purpose of collection), 4(a) (lawful means of collection), 5 (security safeguards), 8 (accuracy to be checked before use) and 9 (information not to be kept longer than necessary). Accordingly, those principles apply in the same way they apply to all agencies subject to the Act.

The 2017 amendment replaces a complete exemption for disclosures *to* intelligence organisations (section 57) with the inclusion of the exception to principle 11, just quoted. The replacement of the complete exemption with an exception means that the Privacy Act can apply in the usual way to require agencies to satisfy themselves that any disclosure that they make falls within the confines of principle 11 and to be able to justify their actions to the Privacy Commissioner in the event of a complaint.

(A related development beyond the Privacy Act itself, is the inclusion of new procedural protections for the business records of telecommunication network operators and financial service providers due to come into force in September. Requests for these business records formerly fell within the Privacy Act exemption (section 57). The business records of companies in either class, including customer information, bank account and transaction details, IP addresses and call associated data must now be sought by the intelligence agencies in accordance with a statutory approval process, jointly supervised by the relevant government Minister and the Commissioner of Intelligence Warrants. The privacy impact is one of the matters considered in granting the approval. The Directors-General of the intelligence agencies must maintain registers of all business record directions, which can then be accessed by the Inspector-General of Intelligence and Security.)

The effect of the changes

The changes to the Act in effect replace a specific exemption with a much narrower exemption combined, in the case of use and disclosure obligations, with an authorisation for use and disclosure. The change in law may appropriately be characterised as a strengthening of the legal standards for the protection of personal data in New Zealand both with respect to:

- agencies disclosing personal information to intelligence organisations, where new limits are expressed in law bringing associated accountabilities, and
- the intelligence organisations themselves – where additional privacy principles are applied with associated statutory responsibilities and accountabilities.

3. Other statutory developments

There are no other significant statutory developments to draw to you attention in this period.

4. Other developments

In the first report submitted in this series in December 2015, as amplified in the supplementary report of March 2016, an account was given in relation to sections 25A and 25B of the Government Communications Security Bureau Act.

Section 25A, it was explained, imposed an obligation on GCSB to formulate a policy on personal information that accorded with 'Principles to protect personal information' set out in section 25B. It was noted in the earlier reports that the section 25B principles were modelled upon several of the information privacy principles in the Privacy Act that are not directly applied to the intelligence organisations (although as reported above shortly are to be applied directly). It was also noted that

the GCSB is required to consult with both the Inspector-General of Intelligence and Security and the Privacy Commissioner in formulating its policy.

By way of update, I can advise that GCSB has declassified and published its policy statement PS-131 "Personal Information Policy for Information Collected for Operational Purposes", July 2016, to give effect to its statutory obligations.

5. Further information and reports

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.

In due course, this report will be published on the website of the Office of the Privacy Commissioner.

It is anticipated that the next periodic report will be provided in December 2017 or thereabouts.