Periodic Update Report on Developments in Data Protection Law in New Zealand

(July – December 2020)

Twelfth Report to the European Commission

By the Competent Supervisory Authority

For the Application of the Legal Data Protection Standards

In New Zealand

29 January 2021

Table of Contents

Privacy Commissioner
Te Mana Mātāpono Matatapu

29 January 2021

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 12th report[1] 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 8 July 2020.

I am pleased to report on four developments in this period. Firstly, the Privacy Act 2020 came into force on 1 December 2020. This update of New Zealand's privacy legislation affirms and enhances the level of data protection in New Zealand. The key changes are summarised in brief in this report.

Secondly, the six Codes of Practice made under the Privacy Act 1993 were repealed and replaced to reflect changes in the new Privacy Act 2020, with effect from 1 December 2020.

Thirdly, an Order in Council has been made under Part 9A of the Privacy Act 1993, approving an information sharing agreement that came into force on 1 October 2020, and revoking an earlier Order.

Fourthly, the New Zealand Court of Appeal issued a unanimous decision in *Dotcom v Attorney-General* [2020] NZCA 551, affirming the Privacy Commissioner's submissions in relation to the interpretation of provisions of the Privacy Act 1993 in relation to the individual's right to seek access to their personal information.

Otherwise, nothing has changed in the last 6 months. In essence, the report simply confirms that the level of data protection in New Zealand is enhanced by the Privacy Act 2020 and has not been diminished during this period. I trust that this is reassuring for the purposes of the Commission's monitoring of the level of data protection under New Zealand law.

[1] Earlier reports are available at https://privacy.org.nz/news-and-publications/reports-to-parliament-and-government/reports-on-new-zealand-adequacy-to-the-european-commission/

I am aware that the New Zealand Government, via the Ministry of Justice, has separately responded to specific questions about New Zealand's Privacy Act 2020. I trust that this brief general overview of developments in the last six months will, together with that other detailed response, assist in your monitoring of the level of data protection under 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.[2] This decision was later amended by a European Commission decision of 16 December 2016 reflecting aspects of the ECJ decision in the first *Schrems* judgment.[3]

The Commission has a responsibility to monitor the functioning of the decision. To assist the Commission 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' under the Commission's decision 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 surveyed developments since the commencement of the Commission's decision in 2013. That initial report was updated by other reports dated 2 March (supplement), 30 June and 9 December 2016, 26 June and 22 December 2017, 9 July and 21 December 2018, and 5 July 2019 and 19 December 2019, and 8 July 2020. This report covers the period July to December 2020 (inclusive).

Regulation (EU) 2016/679 of 27 April 2016 (known as the General Data Protection Regulation or GDPR) came into effect on 25 May 2018 and repealed the 1995 Directive. However, GDPR Article 45(9) provides that the decisions adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC continues in force until amended, replaced or repealed by a Commission decision adopted in accordance with GDPR Article 45(3) or (5). Accordingly, the Commission's adequacy decision covering New Zealand will continue 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 2020. The Act covers the entire public and private sectors, with a few specific public interest exemptions that one might expect in a democratic society.

I am pleased to report that the Privacy Act came into force on 1 December 2020 and is available here. I understand that the Ministry of Justice has briefed you on the law reforms

[2] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013D0065
[3] See C/2016/8353 Commission Implementing Decision (EU) 2016/2295 of 16 December 2016 amending Decisions 2000/518/EC, 2002/2/EC, 2003/490/EC, 2003/821/EC, 2004/411/EC, 2008/393/EC, 2010/146/EU, 2010/625/EU, 2011/61/EU and Implementing Decisions 2012/484/EU, 2013/65

introduced by the Privacy Act 2020. My Office has produced a range of resources to explain and support the new Privacy Act that are available here.

Overall, the new Privacy Act affirms and enhances the level of data protection in New Zealand. The new Act retains all of the information privacy principles with some changes. Principle 1 has been clarified to ensure that businesses and organisations do not collect identifying information from people if it is not necessary. Principle 4 now emphasizes that the circumstances of children and young people are to be considered when collecting their personal information. New information privacy principle 12 has been added and applies when personal information is disclosed to an overseas entity not subject to the Privacy Act.

In brief, other key changes include:

- clarifying the Act's jurisdiction and application to overseas agencies (sections 4, 8 and 9);
- empowering the Privacy Commissioner to issue an access direction requiring an agency to provide an individual with access to their personal information (sections 91 and 92);
- introducing mandatory notification of serious privacy breaches to the Privacy Commissioner, and potentially to affected individuals (Part 6(1));
- empowering the Privacy Commissioner to issue compliance notices for breaches of the Privacy Act or a Code of Practice (Part 6(2));
- introducing criminal offences (punishable by a fine of up to $10,000) for misleading an agency to obtain someone else's personal information, and for destroying personal information where an access request has been made for it (section 212).

The new Privacy Act has clarified some of the refusal grounds where an individual seeks access to their own personal information. There are now express refusal grounds if there is a significant risk of serious harassment, or where releasing information would significantly affect a victim of an offence, or would pose a serious threat to the life, health or safety of an individual, or to public health or public safety.

If a privacy complaint is investigated but not resolved, the individual may commence proceedings in the Human Rights Review Tribunal, now subject to a six month time limitation (section 98). A complaint may be filed by the representative of a class of complainants, and the Tribunal may award damages of up to $350,000 per individual (section 103(2)). There is provision to encourage resolution by limiting the admissibility of apologies (section 100).

One matter that has not been carried over into the new Privacy Act, on the recommendation of the Privacy Commissioner, is the set of four public register privacy principles, as these were outdated. The regulation of personal information contained in public registers will continue to be governed by the statute establishing the public register. These statutes generally provide a right of complaint to the Privacy Commissioner for searches of public registers that do not comply with the provisions of the relevant statute.

In addition, the government information matching provisions in Part 7(4) of the new Privacy Act have been grandfathered so that they continue to apply only to existing information

matching programmes (Schedule 7). Government information sharing by authorised information sharing agreements is now governed by Part 7(1) of the Privacy Act.

Privacy Act Codes of Practice

The 6 Codes of Practice issued under the Privacy Act 1993 were repealed and replaced under the Privacy Act 2020 to reflect changes in the new Privacy Act 2020, with effect from 1 December 2020.

Information about the revised Codes of Practice is available here.

Part 9A Authorised Information Sharing Agreements

The first and second reports in this series of periodic updates explained the operation of Part 9A inserted into the Privacy Act 1993 in 2013 that provides for 'approved information sharing agreements' (known as AISAs) that can be approved by Order in Council from time to time. This has been carried over into Part 7(1) of the Privacy Act 2020. The mechanism for a representative agency to represent a class of agencies has been modified to allow an information sharing agreement to specify one or more classes of agencies that the agreement may apply to.

Part 7(1) includes relevant process safeguards to ensure that any agreement does not unreasonably impinge on the privacy of individuals and contains adequate safeguards to protect their privacy. The development of an AISA requires a Privacy Impact Assessment. The approval process has a number of system checks including consultation with the Privacy Commissioner and relevant groups and stakeholders, ministerial recommendation after taking into account consultation submissions and a set of statutory considerations, authorisation by the Executive, ongoing reporting and Privacy Commissioner review.

Summary details of each AISA are included in Schedule 2 to the Privacy Act 2020.

There was one AISA approved in this period:

- Privacy (Information Sharing Agreement between Inland Revenue, New Zealand Police, New Zealand Customs Service, and Serious Fraud Office) Order 2020 commencing 1 October 2020. This revokes the Privacy (Information Sharing Agreement between Inland Revenue and New Zealand Police) Order 2014. The Order is to continue to authorise the sharing of personal information between Inland Revenue and the New Zealand Police, and to add additional participating law enforcement agencies (New Zealand Customs Service and the Serious Fraud Office). This is to facilitate the maintenance of public safety and law enforcement and crime prevention. Inland Revenue may share personal information with a participating law enforcement agency on request or proactively if there are reasonable grounds to suspect the person has committed or will commit a serious crime (punishable by a term of imprisonment of 4 years or more), including personal information about certain people associated with a suspect (associates, domestic partners and participants in financial relationships). Inland Revenue may share personal information including tax information, financial transaction information and information about assets, employment and personal record information and social assistance information.

Clauses 10 and 11 of the Order sets out the thresholds for sharing personal information under the agreement that requires Inland Revenue to be satisfied that the scope of the information to be shared is limited to that which is necessary in the circumstances, and that it is reasonable, necessary and in the public interest to provide the information to the law enforcement agency.

3. Other statutory developments

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

4. Significant court cases

In the New Zealand legislative scheme for privacy and data protection, individuals do not need to use the courts to enforce their rights. Instead, individuals generally bring complaints to the Privacy Commissioner for resolution at no cost. Nonetheless relevant cases can come before the courts. For instance, Privacy Act cases that are not resolved through the Commissioner's processes can be taken to the Human Rights Review Tribunal which is part of New Zealand's system of specialist statutory tribunals. Cases can be appealed from the Tribunal through the court system.

A recent appeal to the New Zealand Court of Appeal in Dotcom v Attorney-General, is relevant in affirming the level of data protection during the period under review, specifically in relation to the individual's entitlement to request access to their personal information. There have been numerous legal proceedings in New Zealand in relation to Mr Dotcom's extradition sought by the United States. This Privacy Act appeal relates to handling of Mr Dotcom's information privacy requests under principle 6 made ahead of Mr Dotcom's extradition eligibility hearing.

The background to the appeal was that in July 2015 Mr Dotcom sent information privacy requests under the Privacy Act to all Ministers of the Crown and most government departments and agencies asking for all personal information held by them. Citing section 37 of the Privacy Act 1993, he requested that these be dealt with urgently. The majority of the requests were transferred to the Attorney-General. They were then rejected on the basis they were vexatious on account of them all being required urgently.

Mr Dotcom brought proceedings in the Human Rights Review Tribunal alleging an interference with his privacy. The Tribunal's finding of an interference with Mr Dotcom's privacy was overturned on appeal to the High Court. Mr Dotcom was granted leave to further appeal on two questions of law. The Privacy Commissioner was represented in the appeal as intervenor. The decision of the Court of Appeal overturned the High Court decision.

This appeal decision addresses questions about the procedure for transferring access requests under the Privacy Act, and the significance of urgency being sought as a factor in determining if the requests are vexatious (and can therefore be refused). The Court agreed with the Privacy Commissioner that transferring an information privacy request is permissible only if the person dealing with the request believes the information to which the request relates

to be more closely connected with the functions or activities of the transferee agency. The fact that a requester has asked for information urgently is not information to which the information request relates and does not provide a proper basis for a transfer.

Additionally, the Court held that the mere fact of a request for urgency would not generally provide a proper basis for finding an information request to be vexatious, although in some circumstances an inference of vexatiousness could be possibly be drawn from a request for urgency, such as where there are a grossly excessive number of requests for urgency or the reasons given for urgency are not credible. This would always depend on the context in which the request for urgency was made.

This appeal raised a question about the proper interpretation of the Privacy Act 1993. The Court of Appeal agreed with the Privacy Commissioner's submission that the Privacy Act 1993 prescribes legal standards and upholds basic human rights and constitutional standards in respect of information held by public bodies. Parts 4 and 5 of the Privacy Act (the procedural provisions for dealing with access requests, including the transfer provision) are subject to usual principles of statutory interpretation, rather than a more fluid approach that might be suitable in relation to other privacy principles (as argued for the Attorney-General). These procedures ensure that an agency receiving an access request is focused on the request and on the information sought in accordance with the rights that underpin the Act.

The Court held that this right is not susceptible to a more liberal interpretative treatment and that Parts 4 and 5 of the Privacy Act should be construed in accordance with orthodox statutory interpretation.

This is because section 11 of the Privacy Act 1993 gives distinct and legally binding status to the right of access under principle 6, where information is held by public bodies. While section 11 only extends to public sector agencies, the Court could see no reason why this orthodox statutory interpretation would not extend to requests to non-public agencies.

5. Other developments

There are no other developments of significance to report.

6. Further information and reports

Further information may be requested from Joanna Hayward, General Counsel, Office of the Privacy Commissioner at joanna.hayward@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 July 2021 or thereabouts.