



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

(July - December 2025)

---

**Twenty second report to the European Commission  
by the competent supervisory authority  
for the application of the Legal Data Protection Standards  
in New Zealand**

24 December 2025

---

# Table of contents

## **Letter of introduction**

1. Background
2. Statutory amendments to New Zealand privacy law
3. Other statutory developments
4. Significant court cases
5. Other developments
6. Further information

24 December 2025

Ms Louisa Klingvall  
Acting Head of International affairs and data flows  
Directorate-General for Justice & Consumers  
European Commission  
Brussels  
**Belgium**

Dear Ms Klingvall

**Update report on developments in New Zealand data protection law**

I submit this 22nd 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 six months since the last report dated 2 July 2025.<sup>1</sup> I am pleased to report on relevant developments during this period.

Firstly, the Privacy Act 2020 has been amended to create a new Information Privacy Principle (IPP) 3A, which enhances transparency requirements for the collection of personal information.

Secondly, the Biometric Processing Privacy Code 2025 has now been issued. This was signalled in the 20<sup>th</sup> report to the Commission.<sup>2</sup> This code of practice creates specific privacy rules for agencies using biometrics and gives individuals confidence about the use of their sensitive personal information.

Thirdly, I have amended the Telecommunications Information Privacy Code 2020 to ensure search and rescue operations are supported by the Code and to keep in line with the operational structure for emergency location information.

Fourthly, various minor, technical and consequential amendments have been made to the Privacy Act, as summarised in this report.

---

<sup>1</sup> Earlier reports are available from the Privacy Commissioner's website – see "[New Zealand - EU data protection adequacy](#)" Office of the Privacy Commissioner <[www.privacy.org.nz](http://www.privacy.org.nz)>.

<sup>2</sup> [Periodic Update Report on Developments in Data Protection in New Zealand](#) (July-December 2024), 13 January 2025.

Aside from the above developments, nothing has changed in the last six months. In essence, this report confirms that the level of data protection in New Zealand has not been diminished during the review period.

I trust that this update report is reassuring for the purposes of the Commission's ongoing monitoring of the level of data protection under New Zealand law.

Yours sincerely



Michael Webster  
**Privacy Commissioner**  
**New Zealand**

## Background

- 1 On 19 December 2012, the European Commission formally decided that for the purposes of Article 25(6) of Directive 95/46/EC, New Zealand is considered as ensuring an adequate level of protection for personal data transferred from the European Union.<sup>3</sup> 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.<sup>4</sup>
- 2 Regulation (EU) 2016/679 of 27 April 2016, or the General Data Protection Regulation (**GDPR**), came into effect on 25 May 2018 and repealed the 1995 Directive. 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 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 continued under the new GDPR regime.
- 3 On 15 January 2024, following the first review of this adequacy decision, the Commission determined that New Zealand continues to ensure an adequate level of protection for personal data transferred from the European Union.
- 4 The European Commission has a responsibility to monitor the functioning of the decision. To assist the European 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 European Commission’s decision, has undertaken periodically to submit update reports on developments in New Zealand data protection law.<sup>5</sup>
- 5 On 22 December 2015, the Privacy Commissioner submitted the first report that surveyed developments since the commencement of the Commission’s decision in 2013. The Privacy Commissioner submitted subsequent reports dated 2 March 2016 (supplement), 30 June 2016 and 9 December 2016, 26 June 2017 and 22 December 2017, 9 July 2018 and 21 December 2018, and 5 July 2019 and 19 December 2019, 8 July 2020, 29 January 2021, 9 July 2021, 31 January 2022, 4 July 2022, 30 January 2023, 3 July 2023, 2 February 2024, 15 July 2024 and 13 January 2025 and 2 July 2025.
- 6 The Office of the Privacy Commissioner does not, and does not purport to, speak for the New Zealand Government in this report.

---

<sup>3</sup> [2013/65/EU](#): 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).

<sup>4</sup> 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](#).

<sup>5</sup> 2013/65/EU, above n 3.

## Statutory amendments to New Zealand privacy law

- 7 The legal standards for the protection of personal data in New Zealand are primarily set out in the Privacy Act 2020 that came into force on 1 December 2020. The Privacy Act covers the entire public and private sectors, with a few specific public interest exemptions that one might expect in a democratic society.
- 8 During the period of this report, the Privacy Act was amended as a consequence of the [Privacy Amendment Act 2025](#). The key amendment was the addition of IPP 3A in section 22 of the Act. Under IPP 3A, if an agency collects a person's personal information from someone other than the person themselves (i.e. indirectly), then that agency is required to take reasonable steps to ensure the person is aware of that collection, unless an exception applies. This new principle will come into force on 1 May 2026.
- 9 The enactment of IPP 3A improves transparency for individuals about the collection of their personal information and better enables individuals to exercise their privacy rights. The Office of the Privacy Commissioner has also [developed guidance](#) to support agencies in implementing the new principle.
- 10 The Privacy Amendment Act also made technical amendments to the Privacy Act, in brief these include:
  - Clarifying that when giving advice on request to the Minister of Justice about the privacy laws of other countries, the Privacy Commissioner may assess the privacy laws on an individual basis or on the basis of the country being a member of a bloc of countries (sections 18 and 214).
  - Clarifying the withholding ground in section 49(1)(c) to permit an agency to decline to give an individual access to their personal information if the disclosure of the information would be contrary to the interests of any other individual under the age of 16 years to whom the information also relates.
  - Clarifying the withholding ground in section 49(1)(d) to permit an agency to decline to give an individual access to information if disclosure of that information would be likely to prejudice the safe custody or rehabilitation of any other individual to whom the information also relates who has been convicted of an offence or is, or has been, detained in custody.
  - Clarifying that agencies are not required to respond to an access or correction request, if that request has been transferred to another agency (sections 44 and 63).
- 11 The [Parliament \(Repeals and Amendments\) Act 2025](#) made one amendment to the definition of a “New Zealand agency” in section 8 of the Privacy Act. While the Parliamentary Service is a New Zealand agency subject to the Privacy Act (apart from employee information), this recent amendment excludes personal information collected

by a parliamentary security officer under Part 7 of the Parliament Act 2025 with the effect that this information is not subject to the Privacy Act.<sup>6</sup>

- 12 The [Crimes \(Countering Foreign Interference\) Amendment Act 2025](#) created new offences, with a consequential amendment to section 90 of the Privacy Act. Section 90 provides that the Commissioner and their employees can be compelled to give evidence in court as to matters that came to their knowledge through performing their functions, only in relation to proceedings for specific criminal offences.
- 13 The [Statutes Amendment Act 2025](#) made minor technical amendment to the Privacy Act; in brief these include:
  - Clarifying that IPP 12(1)(e) enables the disclosure of personal information to a foreign person or entity if the recipient is subject to the laws of a country assessed to have privacy laws with comparable safeguards and that disclosure is not precluded by a limitation or qualification prescribed in regulations (sections 22 and 214).
  - Clarifying section 27 that IPPs 5 to 12 do not apply to an individual who is holding personal information collected by a lawful means solely for the purpose of that individual's personal or domestic affairs, including when the personal information was received by that individual unsolicited or created by that individual.
  - Clarifying that a reason for refusing access to personal information under section 53 is where the information is not readily retrievable, in respect of which the requestor will have a right to complain to the Privacy Commissioner.
  - Clarifying that an agency may refuse a request to access personal information if disclosure of the information would be likely to prejudice the health of the individual concerned (section 49(1)(b)).
  - Confirming the Privacy Commissioner's discretion to decline to investigate a complaint if an investigation is inappropriate in the circumstances (section 74(2)).
  - Clarifying that, following an investigation, the Privacy Commissioner has the discretion to use best endeavours to secure settlement of a complaint and an assurance from the respondent that the action giving rise to the complaint will not be repeated, when it is appropriate to do so (sections 91 and 94).
  - Clarifying when the limitation period for bringing proceedings in the Human Rights Review Tribunal commences where there are related complaints or matters being considered by the Privacy Commissioner or the Director of Human Rights Proceedings (section 98).

---

<sup>6</sup> Part 7 of the Parliament Act 2025 sets out the powers and duties of parliamentary security officers including search and seizure powers and the power to deny entry to parliamentary precincts.

- Clarifying who is an agent for purposes of sections 120 and 121 of the Privacy Act that concerns the liability provisions for an agency's privacy breach notification obligations.

## Codes of Practice

- In the twelfth report to the European Commission, the Privacy Commissioner confirmed that the six 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.<sup>7</sup> Information about the revised Codes of Practice is available on our website [here](#).
- Following public consultation, the Privacy Commissioner has issued the [Biometric Processing Privacy Code](#) that creates specific privacy rules for agencies using biometric technologies to collect and process biometric information. The Code came into force on 3 November 2025 for new users of biometrics. Agencies already using biometrics must comply with the Code from 3 August 2026. The Office of the Privacy Commissioner has [developed guidance](#) to assist agencies to comply with their obligations under the Biometrics Code.
- The Code requires agencies to assess the effectiveness and proportionality of using biometrics, adopt safeguards to reduce privacy risk, and tell people a biometric system is in use, before or when their biometric information is collected. It also limits some particularly intrusive uses of biometric technologies, for example, using them to predict people's emotions or infer information like ethnicity or sex, or other information protected under the Human Rights Act 1993.
- The Privacy Commissioner also [amended](#) the Telecommunications Information Privacy Code (**TIPC**) to support search and rescue operations by explicitly allowing for an emergency service provider to share location information with volunteers or others working on its behalf for the limited purpose of supporting a search and rescue operation. This amendment came into force on 8 December 2025.
- The TIPC was also amended to align with the new operational structure for emergency location information. Minor technical amendments were also made.

## ***Part 7(1): Approved information sharing agreements***

- The first and second reports in this series of periodic updates explained the operation of that part of the Privacy Act (now Part 7, subpart 1) that provides for 'approved information sharing agreements' (known as **AISAs**) that can be approved by Order in Council from time to time.

---

<sup>7</sup> 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 (Privacy Commissioner of New Zealand, 29 January 2021) at 7.

20 Part 7, subpart 1 of the Privacy Act sets out relevant process safeguards to ensure that an AISA does not unreasonably impinge on the privacy of individuals and contains adequate safeguards to protect their privacy. For example, the Privacy Act requires agencies to undertake a privacy impact assessment when developing an AISA. 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, and ongoing reporting and Privacy Commissioner review. You can review the summary details of each AISA in [Schedule 2 of the Privacy Act](#).

21 No further AISAs have commenced in this period.

### **Other statutory developments**

22 There are no other significant statutory developments to draw to your attention in the Review Period.

### **Significant court cases**

23 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 to that individual.

24 Nonetheless, some parties may still choose to bring relevant privacy cases to the courts. For instance, 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. Parties may also use the vehicle of judicial review to challenge a public sector agency's decision with respect to personal information.

### **Other developments**

25 There are no other developments of note during this period that I draw to your attention.

### **Further information and reports**

26 If you have any further questions or would like further information please contact Joanna Hayward, General Counsel, Office of the Privacy Commissioner at [joanna.hayward@privacy.org.nz](mailto:joanna.hayward@privacy.org.nz).

30 In due course, we will publish this report on the website of the Office of the Privacy Commissioner at [www.privacy.org.nz](http://www.privacy.org.nz).

31 It is anticipated that the next periodic report for the period January to June 2026 will be provided in July 2026.