



# Annual Report 2024/25



# Annual Report of the Privacy Commissioner

for the year ended 30 June 2025

Presented to the House of Representatives pursuant  
to section 150 of the Crown Entities Act 2004.

## **The Minister of Justice**

I submit my report as Privacy Commissioner  
for the year ended 30 June 2025.

# Contents

2	Introduction from the Privacy Commissioner
5	Statement of responsibility
6	We are committed to promoting privacy
7	2024/25: privacy in numbers
8	Our strategic framework
9	Tuitui kākahu, tuitui tāngata
10	The privacy system is broad and challenging
11	Privacy benefits all New Zealand
13	New Zealand needs Privacy Act modernisation
14	Our funding continues to be limited
15	We undertake a wide range of functions
16	We focused on three key things in 2024/25

## 17 Strategic objectives progress | Te kauneke ki ngā whāinga rautaki

18	Our progress towards our objectives and privacy outcomes
19	Objective 1: We will work in partnership with Māori to take a te ao Māori perspective on privacy
24	Objective 2: We will engage and empower people and communities who are more vulnerable to serious privacy harm
29	Objective 3: We will set clear expectations to provide agencies with greater certainty about their responsibilities
34	Objective 4: We will promptly use our full range of investigation and compliance powers to hold agencies accountable for serious privacy harm

## 40 Office and functions | Te Tari me āna mahi

41	Independence and other interests
41	Reporting
41	Staff
42	Statutory Remuneration Disclosures
42	Employees Remuneration
43	EEO Profile

## 44 Finance and performance report | Pūrongo whakahaere pūtea me ngā tutukitanga

45	Statement of performance
46	PBE FRS 48 Service performance reporting
47	Statement specifying comprehensive income
48	Cost of service statement
50	Performance against statements of service performance
50	Function 1: Strategy and insights
51	Function 2: Communications and education
52	Function 3: Compliance and enforcement
53	Function 4: Advice and advocacy
54	Function 5: Investigations and dispute resolution
55	Statement of accounting policies
57	Statement of comprehensive revenue and expenses
58	Statement of changes in equity
59	Statement of financial position
60	Statement of cash flows
61	Notes to the financial statements

## 71 Appendices | Ngā Tāpiritanga

71	Appendix A   Tāpiritanga A
88	Appendix B   Tāpiritanga B

# Introduction from the Privacy Commissioner

As I reflected on the range of initiatives and activity set out in this year's Annual Report, I was struck by a particular thought – that is, the need to re-frame the language of privacy, and protecting and respecting personal information.

We need to break what I call the false dichotomy narrative – that we live in a world of either/or. That you can either have public safety or privacy. That you can either have law and order, or maintain a right to privacy. That you can either have technological innovation or privacy. That you can either embrace AI within your organisation or protect and respect personal information.

I believe we need to own and communicate that privacy is not an either/or – but that it's an “and”, or a “while”. We need to stress this in the language we use, in addressing complex public policy problems, and in developing new business strategies. It's things like keeping people safe while protecting individuals' privacy rights. It's rolling out AI in the health sector and ensuring sensitive personal health information remains protected. It's implementing biometric processing technology, while giving people confidence it's being done safely and fairly. It's doing privacy well.

The Inquiry into Foodstuffs North Island's trial use of Facial Recognition Technology (FRT) saw this Office develop important expectations around how privacy can be protected while using such privacy intrusive technology. The trial findings will help other businesses to ask the right questions about whether FRT is necessary and appropriate for them, and to understand what they would need to do to set FRT up and run it in a privacy protective way.

The delivery and implementation of the Biometric Processing Privacy Code strengthens and clarifies the privacy protections relating to sensitive biometric information. It provides agencies with a legal framework for how to implement biometric technologies. The Code, supported by detailed guidance, ensures businesses and organisations understand how to do privacy well when using these technologies.

The right to privacy is one of our nation's taonga. A society that values privacy is one where its people can have confidence that their personal information will be protected and respected. We have a way to go but we're making progress. That's especially true when I reflect on how my Office, as regulator, has been clear and fair in working with businesses and public sector agencies looking to introduce new ways of delivering on their objectives.

The Statement of Intent 2023–2027, sets out my Office's purpose as, 'ensuring that privacy is a core focus for agencies'. We do this to protect the privacy of individuals, enable agencies to achieve their own objectives, and safeguard a free and democratic society.

This Annual Report marks the second year in our push towards achieving four objectives:

- 1 Work in partnership with Māori to take a te ao Māori perspective on privacy.
- 2 Engage and empower people and communities who are more vulnerable to serious privacy harm.
- 3 Set clear expectations to provide agencies with greater certainty about their responsibilities.
- 4 Promptly use our full range of investigation and compliance powers to hold agencies accountable for serious privacy harm.

### It's been a successful year

We are a nimble Office staffed by people who care deeply for the rights of New Zealanders and who work well together to deliver results.

Significant highlights include the following:

- Developing and then issuing the Biometric Processing Privacy Code to ensure clarity and a legal framework around the automated use of biometric technologies. We're helping keep New Zealanders' sensitive personal information safe while allowing businesses and organisations to innovate. We know that legislation can be a challenge to interpret so we also wrote specific and detailed guidance to help people understand how the new rules apply to them and their business.
- We found that the live Facial Recognition Technology model trialled by Foodstuffs North Island is compliant with the Privacy Act 2020. As well as delivering the results of our Inquiry, our report showed any business considering or using FRT what they need to do to make sure they set things up right to stay within the law.
- At its heart, privacy is about people and we've delivered a range of guidance, or draft guidance for public feedback on topics like biometrics, health, and the upcoming new indirect notification principle that was drafted and consulted on as part of the Privacy Amendment Bill. We support this work by speaking to audiences across the motu, ensuring technical subjects are explained in a way that is understandable.
- Our Māori Reference Panel was established this year. We are now fortunate to work with a group of experts who bring a te ao Māori perspective to our work. Their work helps us engage effectively with Māori to ensure policy projects and other significant work programmes appropriately consider te ao Māori perspectives.
- We received and processed 1,598 complaints from people across New Zealand, in many cases, finding that they had experienced harm from privacy breaches. We also negotiated financial reparation for 6.5% of the privacy complainants that we accepted for consideration.
- This year 1,093 privacy breach notifications were notified to us. Our team provided advice and guidance to organisations and helped them manage what had gone wrong, which then helped people who'd been affected by those breaches.
- We reviewed the Government's legislative programme as it was progressed and made 12 submissions to Select Committees during the year to ensure privacy was considered. We also provided sound privacy advice to dozens of agencies which helped them strengthen their policy projects.

- People want to do privacy well but sometimes need help to understand how that happens. We've written guidance about protecting the privacy of children and young people when taking photos and videos, and created privacy posters in English and te reo Māori to ensure students, educators, and parents understand how to protect children's privacy. We also progressed the other guidance in our Children's Privacy project, which will be available online.
- Privacy Week 2025 was a highlight in May for us. More than 8,500 viewers watched 21 free webinar options with topics like AI, children's privacy, and Māori data sovereignty.
- We hosted the 63<sup>rd</sup> Asia Pacific Privacy Authorities Forum, a virtual meeting of 14 privacy authorities in the Asia Pacific region. Talking to our counterparts, and hearing from them, helps us gain new insights and ideas into how to do privacy well.
- The New Zealand Supreme Court released its majority decision in *Tamiefuna v R*, a case in which we had made privacy submissions as an intervener, and with the Court taking notice of our 2022 joint report with the Independent Police Conduct Authority on Police photography of members of the public.

It's been a great year for demonstrating the value of privacy. I want to thank and congratulate everyone in my Office who has worked hard to help New Zealanders understand why privacy matters so much to people, business, and society.

## **New Zealanders want their privacy rights respected and protected**

More and more New Zealanders know they have privacy rights and want to do something about that. In this year's privacy survey of over 1,000 New Zealanders, we learnt that 82% of people wanted more control and choice over the collection and use of their personal information.

In a single year there has been a significant jump in how many privacy complaints we've received. This year it's up 21% on the year before.

This year we also had a 27% increase in privacy breach notifications. It's clear that agencies need to respond to the challenge to be better at safeguarding New Zealanders' personal information.

My Office will continue championing the privacy rights of New Zealanders. We will continue to take a constructive approach to the opportunities and challenges that New Zealand organisations and businesses are navigating. We will continue to advocate for changes to make the Privacy Act 2020 fit-for-purpose in the digital age.

I look forward to what we will achieve in 2025/26.



**Michael Webster CVO**  
**Privacy Commissioner**



# Statement of responsibility

Under the Crown Entities Act 2004, the Privacy Commissioner is responsible for the preparation of the financial statements and statement of performance, and for the judgements made in them.

We are responsible for any end-of-year performance information provided by the Privacy Commissioner under section 19A of the Public Finance Act 1989.

The Privacy Commissioner has the responsibility for establishing and maintaining a system of internal control designed to provide reasonable assurance as to the integrity and reliability of financial and performance reporting.

In the opinion of the Privacy Commissioner, these financial statements and statement of performance fairly reflect the financial position and operations of the Privacy Commissioner for the year ended 30 June 2025.



**Michael Webster CVO**  
**Privacy Commissioner**  
24 October 2025



**Emma Boddy**  
**General Manager**  
24 October 2025

# We are committed to promoting privacy



**Michael Webster CVO**  
Privacy Commissioner

Michael was appointed as Privacy Commissioner in July 2022. Prior to his appointment he was the Secretary of the Cabinet and Clerk of the Executive Council of New Zealand, a position he held since March 2014.



**Liz MacPherson**  
Deputy Privacy Commissioner

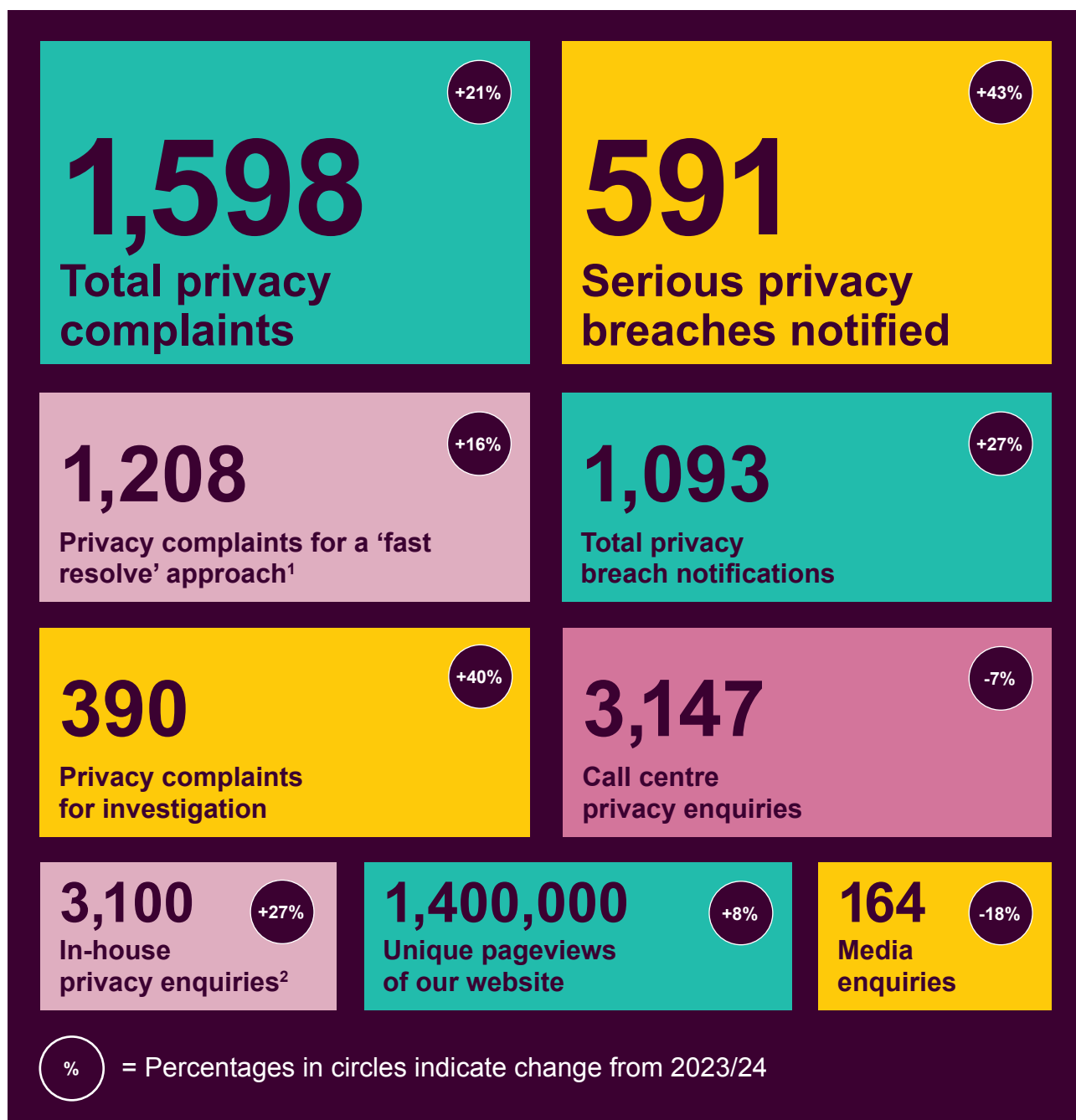
Liz was appointed as the first statutory Deputy Privacy Commissioner in November 2021. Liz first joined the Office of the Privacy Commissioner in April 2020 and previously held several Deputy Chief Executive roles before being appointed to the position of Government Statistician.

**Ko Rangitīkei te whenua tupu**  
**Ko Tāmaki Makaurau te kāinga**  
**Kei Te Whanganui-a-Tara au e mahi ana**  
**Ko ahau te Kōmihana Matatapu**  
**Ko Michael Webster ahau**  
**Tēnā koutou katoa**

**Tena koutou katoa**  
**I whanau mai au i Tāmaki Makaurau**  
**Nō Aerana, Kōtirana, Ingarangi me**  
**Haina ahau**  
**I tupu ake au i Puni, Tokirima, Waiuku,**  
**Waiotira, Te Akau me Waimauku**  
**Kei te Whanganui-a-tara tōku**  
**kāinga ināiane**  
**Ko te Komihana Tuarua ahau**  
**Ko Liz MacPherson tōku ingoa**



# 2024/25: privacy in numbers



1. Note that how 'fast resolve' complaints are identified has been changed in this Annual Report. More information on this change is available on page 36.
2. The change in how 'fast resolve' complaints are identified (see footnote 1) has meant that the number of in-house enquiries in the 2023/24 year decreased to 2,436.

# Our strategic framework

## Our system outcomes



Individuals are more confident that their privacy is protected.

Agencies can better achieve their own objectives through respecting the privacy rights of New Zealanders.

The right to privacy and the protection of personal information is valued in New Zealand.

## Our purpose

We ensure privacy is a core focus for agencies in order to protect the privacy of individuals, enable agencies to achieve their own objectives, and safeguard a free and democratic society.

## Our objectives



We work in partnership with Māori to take a Te Ao Māori perspective on privacy.

We engage and empower people and communities who are more vulnerable to serious privacy harm.

We set clear expectations to provide agencies with greater certainty about their responsibilities.

We promptly use our full range of investigation and compliance powers to hold agencies accountable for serious privacy harm.

## Our functions



Communication and Education



Compliance and Enforcement



Policy and Advocacy



Investigations and Dispute Resolution



Strategy and Insights

## Our values



Respect

+



Integrity

+



Independence

+



Innovation

+



Excellence

# Tuitui kākahu, tuitui tāngata

## The weaving of a cloak, the weaver of people

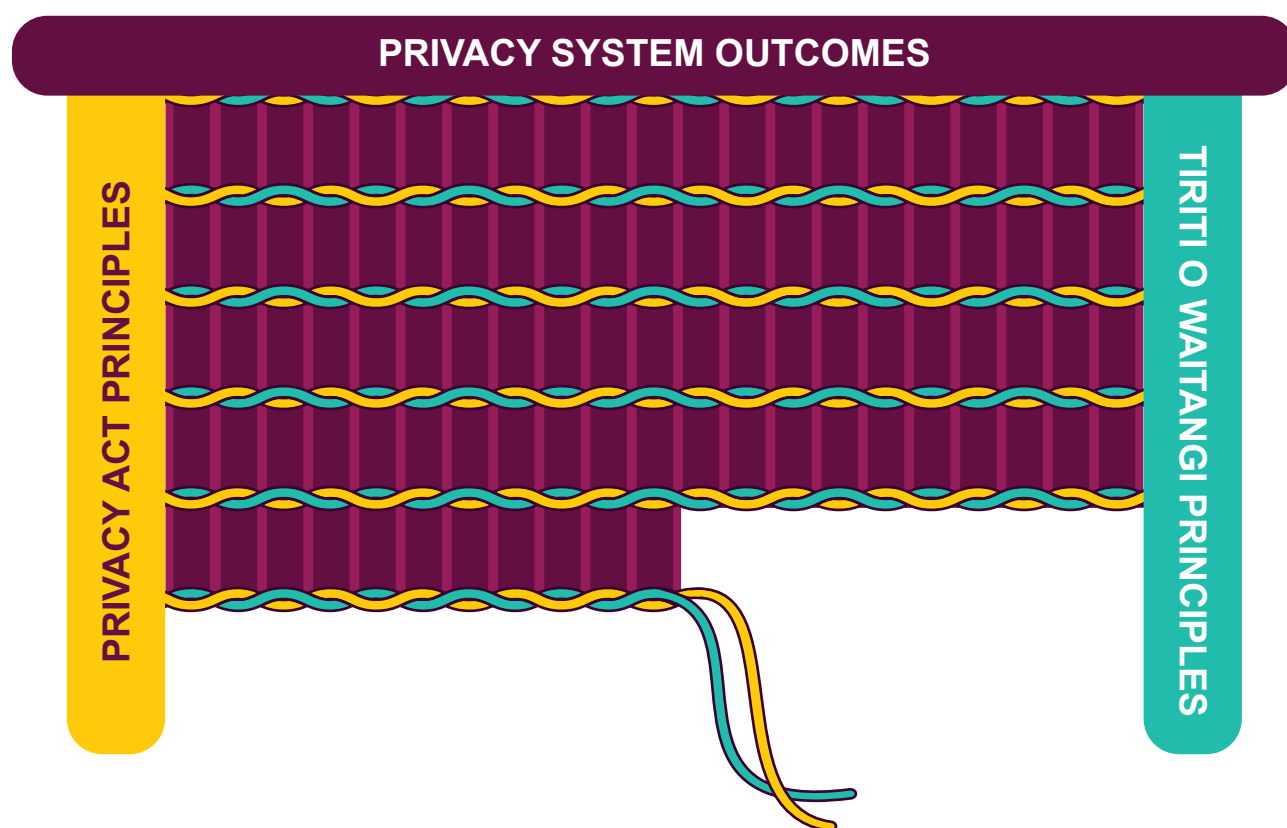
Our Statement of Intent introduced the whakataukī of tuitui kākahu, tuitui tāngata – it speaks to the process of weaving a kākahu or traditional Māori cloak and aligns that to the weaving of people.

It is a whakataukī that works well in describing the privacy system, the role of the Office of the Privacy Commissioner, and the place of Te Tiriti o Waitangi. This includes:

- tiaki – protecting and safeguarding the privacy of all New Zealanders
- taunaki – supporting the aspiration of rangatiratanga as expressed by Māori over their taonga, their data, and their privacy
- tūhono – partnering with Māori.

Tuitui kākahu, tuitui tāngata describes the process of weaving and the completion of the garment, or cloak that can then be used by individuals, whānau, hapū, iwi, and Māori to protect their privacy.

Tuitui kākahu, tuitui tāngata represents how the principles of Te Tiriti o Waitangi and the Act work together to achieve the outcomes of the privacy system.



# The privacy system is broad and challenging

We are the regulator of the privacy system – the flows of personal information between individuals and agencies throughout New Zealand. The figure below illustrates the breadth of the privacy system.

The privacy system is a challenging environment to regulate. There is rapid technological change and keenness to

use technologies such as facial recognition and artificial intelligence. Our regulated sector is very broad, extending to nearly the entire public, private and not-for-profit sectors. Good privacy practice requires every agency to consider their specific situation, and many have a low understanding about how to manage privacy well.

## Key parties in the privacy system

### Wider privacy system

#### Industry bodies

Represent and champion the interests of agencies

#### Privacy advisors

Assist agencies with advice on how to meet privacy requirements

#### ICT providers

Provide agencies with processing or storage capabilities

### Core regulatory system

#### Ministry of Justice

Lead government agency for privacy policy advice

#### Office of the Privacy Commissioner

Regulator of the privacy system

#### Individuals

Individuals have their personal information used by agencies in return for goods and services

#### Agencies

Agencies (public and private) use personal information to achieve their objectives

#### Human Rights Review Tribunal

Judicial body for privacy issues

#### Advocacy groups

Help individuals directly or advocate for privacy improvements on their behalf

#### Māori organisations

Represent Māori interests with a core focus on the success and wellbeing of Māori

# Privacy benefits all New Zealand

We have set our purpose as ‘ensuring that privacy is a core focus for agencies’ because we believe it’s the best way to improve the outcomes of the privacy system. Our interventions are designed to drive improvements to the privacy understanding and capabilities of agencies and to increase the priority and importance of privacy in their decision making.

Our indicators on the performance of the privacy system and privacy outcomes are outlined in the section, ‘Progressing toward our objectives and privacy outcomes’.



**Good privacy practices reduce the likelihood of a breach happening, and if it does occur, they reduce the harms caused by privacy breaches.**

1

## **Individuals are more confident that their privacy is protected**

When people trust that their personal information will be treated as a taonga, it gives them confidence in an agency.

Good privacy practices reduce the likelihood of a breach happening, and if it does occur, they reduce the harms caused by privacy breaches, whether emotional, reputational, financial, or physical. In 2024/25, when we helped settle a privacy complaint with a financial settlement, the average settlement amount was over \$13,000. When the Human Rights Review Tribunal has considered privacy cases this year and determined there should be a financial settlement, the average settlement amount for emotional harm or injury to feelings was over \$21,000.

2

## Agencies can better achieve their own objectives through respecting the privacy rights of New Zealanders

Agencies use the personal information that people give to them to deliver goods or services, either for profit or as a public service.

Privacy breaches create high costs to agencies both in remedying what went wrong and, in some cases, reimbursing customers. It can also impact the ability of the business to deliver products or services, as important data may have been lost, and there could be a loss of existing customers or clients. In our 2025 survey of New Zealander's attitudes to privacy, 67% of respondents said they would likely change service providers if they heard that their provider had poor privacy and security practices.



OF RESPONDENTS SAID THEY WOULD LIKELY CHANGE SERVICE PROVIDERS IF THEY HEARD THAT THEIR PROVIDER HAD POOR PRIVACY AND SECURITY PRACTICES

3

## The right to privacy and the protection of personal information is valued in New Zealand

The outcomes of the privacy system extend beyond the interactions of individuals and agencies.

Collectively, a society that values privacy and personal information is one where its people can have greater trust in government and institutions because they know that the information that is precious to them will be well treated. This trust helps drive better outcomes by encouraging engagement in democratic and consultation processes, helping to inform the design of effective services, and tackling complex problems. This trust is especially important for whānau, hapū, and iwi in achieving their aspirations for fair and just outcomes and data sovereignty. We contribute to this trust through our statutory independence that provides the public with a 'watch dog' who advocates on their behalf.



**Collectively, a society that values privacy and personal information is one where its people can have greater trust in government and institutions.**



# New Zealand needs Privacy Act modernisation

## The need for change is increasingly urgent

The Act is increasingly ‘long in the tooth’ as it is based on Law Commission recommendations from 2011. Many countries have modernised their privacy regimes beyond our own to capture the benefits and avoid the harms of new technologies. For example, some countries have amended privacy legislation or created new legislation to accommodate developments in the field of artificial intelligence.

The Act also provides insufficient incentives for many agencies to understand or meet even the basic privacy requirements, leading to significant non-compliance that is difficult for us to address. For example, a growing number of small-to-medium sized agencies do not establish policies and practices to effectively manage the privacy impacts of their activities or have failed to appoint a privacy officer.

The New Zealand public supports the need for Act reform. In our March 2025 survey of over 1,000 New Zealanders, three quarters of those surveyed considered that the Privacy Commissioner should have the power to audit the privacy practices of agencies, to issue small infringement fines for a privacy breach, and the power to ask Courts to issue large fines for serious privacy breaches.

## The specific amendments we are proposing to the Act

We continue to recommend a specific set of amendments to the Act to the Government that would further modernise it and strengthen privacy outcomes. They include:

- 1 Empowering New Zealanders to better protect themselves with new rights, such as a ‘right to erasure’ that would provide individuals with the right to ask agencies to delete their personal information.
- 2 Establishing strong incentives for agencies to take privacy seriously through establishing a new and significantly stronger penalty regime.
- 3 Requiring agencies to be able to demonstrate how they meet their privacy requirements, such as the privacy management programmes recommended by the OECD.
- 4 Providing New Zealanders with stronger protections for automated decision making, which can have issues with inaccurate predictions, discrimination, unexplainable decisions and a lack of accountability.

# Our funding continues to be limited

Over the past several years there have been multiple changes to our operating grant. The history of our funding is outlined below.

Even when our funding was increased it was to a level below what we had recommended to implement the significant new responsibilities and powers that the Act provided us. Following these increases, high inflation and cost savings measures subsequently diminished our funding in real terms.

We continue to fund a deficit through cash reserves, an approach that can only be maintained in the short term. As cash reserves are reduced, we will need to ensure expenditure reflects our funding levels.

Year	Funding (\$000)	Note
2020/21	7,276	Privacy Act 2020 comes into force
2021/22	7,392	
2022/23	7,392	
2023/24	8,171	Budget 2023 funding increases to support compliance and enforcement
2024/25	7,640	Budget 2024 cost savings decrease
2025/26	7,641	

# We undertake a wide range of functions

## Strategy and Insights

- Using intelligence obtained from our activities across our Office to identify domestic trends and emerging strategic issues
- International insights on emerging privacy issues
- Understanding new trends globally and prioritising delivery of services accordingly
- Monitoring the success of new initiatives and strategies introduced

## Communication and Education

- Guidance and education to empower New Zealanders to exercise their privacy rights and agencies on their responsibilities and obligations under the Act
- Improving digital services channels, including the website and education and guidance tools
- Commenting on issues of public and media interest
- Engagement focused on understanding those parts of society more vulnerable to serious privacy harm

## Compliance and Enforcement

- Receiving breach notifications and following up with agencies on those likely to cause serious harm
- Issuing guidance to agencies reporting a non-serious privacy harm or risk
- Proactively identifying and investigating systematic issues for possible intervention
- Setting expectation with agencies about privacy practices and, where necessary, compliance orders to address systemic issues
- Applying the Compliance and Regulatory Action Framework

## Policy and Advocacy

- Providing clear expectations for agencies, whether through information, guidance or codes of practice
- Providing advice to the government on emerging and new legislation and policy proposals, applying the principles of necessity and proportionality
- Supporting responsible information sharing including the facilitation of Approved Information Sharing Agreements (AISAs) to assist public agencies to operate more effectively and efficiently
- Treaty and te ao Māori analysis incorporated in policy work as necessary

## Investigations and Dispute Resolution

- Investigating privacy complaints made under the Act and referring appropriate complaints to the Director of Human Rights Proceedings for consideration
- Taking a dispute resolution approach where possible and focusing on settlement
- Issuing access directions where appropriate

# We focused on three key things in 2024/25

In our second year under the Statement of Intent 2023–2027 we pursued three key areas of strategic focus<sup>3</sup>. Our accomplishments related to these areas are contained within the Objectives section of this report.

## Continuing to build our strengthened Compliance and Enforcement function

Our Compliance and Enforcement function directly improves the compliance of agencies with Act requirements.

By doing so, it also sends a clear message to the wider privacy system and incentivises meeting privacy more broadly. We have been prioritising this function in recent years and it is now accomplishing its work to a high standard.

## Delivering on our regulatory stewardship responsibilities

A key aspect of our regulatory stewardship responsibilities is ensuring that our Codes of Practice and guidance are fit-for-purpose.

Through achieving this agencies will have a clearer understanding of the requirements of the Act and will be better able to meet them.

## Ensuring the Privacy Act is fit-for-purpose in the digital age

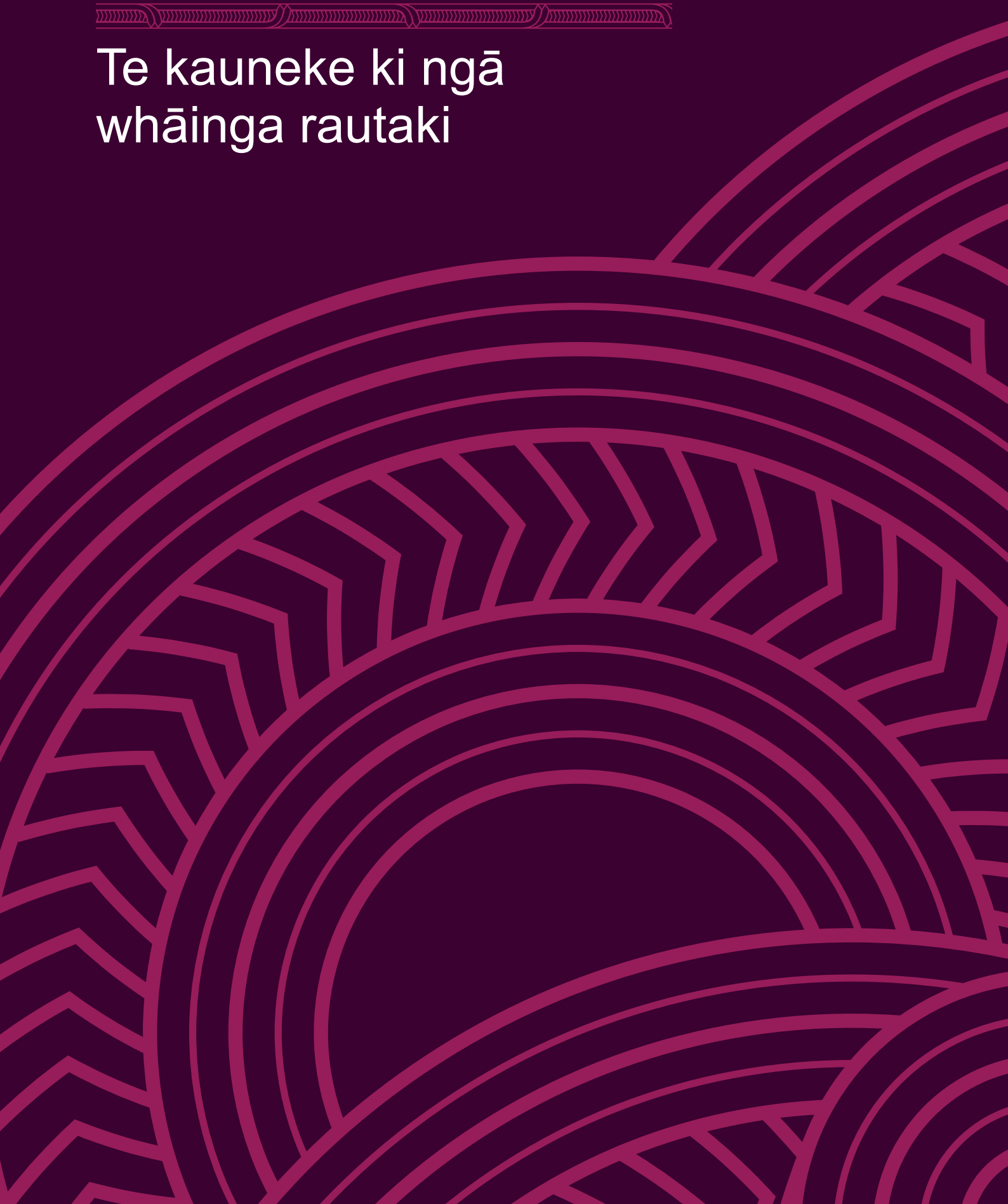
We promote Act reform to better promote New Zealand's privacy outcomes in a changing world.

Another aspect of our work in this area is to support the success of amendments to the Act with our advice to government and guidance to industry.

3. These areas were set in the Statement of Performance Expectations 1 July 2024 to 30 June 2025.

# Strategic objectives progress

Te kauneke ki ngā  
whāinga rautaki



# Our progress towards our objectives and privacy outcomes

Our strategic objectives have been set with the ambition of achieving them over the lifespan of our 2023–2027 Statement of Intent. The objectives will drive us toward being an effective modern privacy regulator who makes privacy a core focus for agencies.

The following sections outline the scope of each objective, what we have achieved so far and the challenges we face. We also include key performance information for the indicators that relate to privacy system outcomes and our objectives.

Measuring privacy outcomes is difficult due to the intangible nature of privacy and because we only see a tiny part of the personal information flows within New Zealand. This means that significant observable operational volumes, such as privacy complaints from individuals, cannot by themselves be used as an indicator of privacy outcomes. For example, an increase in privacy complaints by individuals could be viewed as either an increase in privacy harm or more people being aware of their privacy rights. With these complexities in mind, we have identified some good proxy indicators for privacy outcomes.



**...an increase in privacy complaints by individuals could be viewed as either an increase in privacy harm or more people being aware of their privacy rights.**





## Objective 1:

We will work in partnership with Māori to take a te ao Māori perspective on privacy

This is a cross-cutting objective that all our functions support.

Building our te ao Māori capabilities will enable us to provide more responsive and inclusive services and better connect with Māori and Māori institutions, ranging from hapū to Māori health providers to Māori data sovereignty experts. This will in turn put us in the position to achieve better privacy outcomes for Māori.

Our Office is increasingly expected to have a strong understanding and capabilities relating to the Treaty of Waitangi / Te Tiriti o Waitangi, tikanga Māori and te ao Maori. Section 21(c) of the Act requires the Privacy Commissioner to take account of these perspectives when exercising his functions. We recognise that to be an effective privacy regulator we need to be able to walk in a te ao Māori world and consider privacy through a te ao Māori lens.

Over the period of 2023–2027 the Statement of Intent outlined our ambition to:

- expand the capability and confidence of staff to engage effectively with Māori and in te ao Māori through training in te rēo Māori, tikanga, and kawa
- prioritise empowering Māori to use their privacy rights
- provide the public sector with greater clarity about the application of the Treaty of Waitangi to privacy issues and te ao Māori perspectives on privacy and support all agencies to better understand and accommodate cultural privacy perspectives
- develop strong partnerships with and across te ao Māori and have these partnerships shape our priorities and approach to our work.

## The challenges ahead of us

There are significant challenges for us to take a te ao Māori approach to privacy. We have high expectations about our understanding and capabilities relating to Te Tiriti, tikanga Māori and te ao Māori. These expectations emphasise the importance of putting in the work to make our engagement worthwhile to Māori.

Our biggest challenge continues to be the development of our internal capabilities and during this year we took a new approach to te reo where an online service provider is used with support from internal groups to encourage uptake.

There is an opportunity for us to better gauge how well our functions are reaching Māori and we are exploring the collection of demographic information of individuals who have made privacy complaints to our Office. We consider that the Māori population is more likely to be vulnerable to serious privacy harm due to being disproportionately represented in a range of statistics such as chronic diseases, poverty, and crime. By identifying who we are serving we will be able to lift our engagement, with a focus on promoting understanding about privacy rights.

## Our progress and achievements in 2024/25

We have had some significant achievements over the past 12 months and continued to embed and develop important initiatives that were commenced in the previous year:

- We continued to advance the work of Te Ranga Tautiaki, our Māori reference panel that will enable us to enrich our work with te ao Māori perspectives and make new connections when further Māori engagement is required. This panel meets quarterly and is providing advice on our work programme.
- We continued to upskill staff capability in te ao Māori to better understand a Māori perspective on privacy through our Māori Capability Plan.
- We reached the final stages of our Project Whatu research about the tikanga underpinning the protection of personal information from a Māori perspective. This research will guide the training of our staff and support agencies to take a Māori approach to privacy.



**We consider that the Māori population is more likely to be vulnerable to serious privacy harm due to being disproportionately represented in a range of statistics such as chronic diseases, poverty, and crime.**

## Assessing our impact

Indicator	Māori awareness of right to access personal information under the Privacy Act
Baseline (year)	50% (2022) <sup>4</sup>
Desired change	Increase
<b>2024/25 result</b>	<b>51% (2025)<sup>5</sup></b>
2023/24 result	54% (2024) <sup>6</sup>

This indicator is the closest that we have for measuring the privacy outcomes for Māori. The right to access personal information under the Act is important and awareness of that right is a useful proxy for general privacy understanding. Our ambition is to increase the level of awareness over time.

We measure this indicator through our privacy survey, which surveys over 300 Māori adults each time it is conducted. The results of the 2022 survey found that the level of Māori awareness of their right to access personal information was 50%. The April 2024 result was 54%, a small increase, while the March 2025 result was 51%. With these results to date our conclusion is that Māori awareness of their right to access personal information is being maintained but not increased.

Indicator	All externally reviewed policy files appropriately incorporate Treaty and te ao Māori analysis as necessary
Baseline (year)	New measure
Desired change	Maintain
<b>2024/25 result</b>	<b>Achieved Refer to Function 4 section for details</b>
2023/24 result	Achieved Refer to Function 4 section for details

Every year our policy work is independently audited as a quality assurance check using the government Policy Quality Framework. One aspect of this review is whether our policy work appropriately incorporates Treaty and te ao Māori analysis.

The external review for 2024/25 identified that, although there was limited consideration of te ao Māori perspectives, where it was covered, it was done well. We are satisfied with this result as it maintains what we achieved in 2023/24.

Indicator	Continued implementation of our Mahere Reo strategy and training to develop staff understanding of te ao Māori
Baseline (year)	New measure
Desired change	Increase
<b>2024/25 result</b>	<b>Achieved</b>
2023/24 result	Achieved

As the internal strategy for building te reo skills, our Mahere Reo/Māori Language Strategy is an important driver for our success with this objective. The achievements that we have made include making te reo visible in our office, giving all staff, including leadership, the opportunity to learn te reo online with Reo Ora, promoting te reo in our greetings and publications and measuring progress of learners with te reo. These initiatives also extend to waiata practice, learning about Māori culture through Reo Ora, engaging in staff activities for Māori Language Week and Matariki, participating in an annual wānanga for all staff and mihi whakatau for new employees.

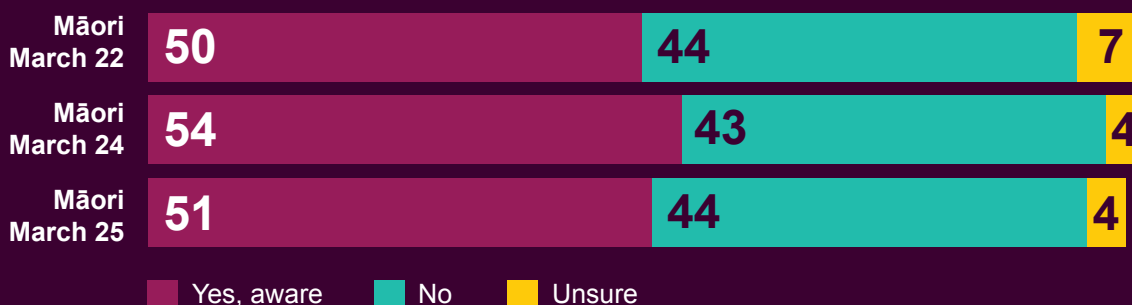
4. *Privacy concerns and sharing data, Omnibus research commissioned by the Privacy Commissioner.* AK Research & Consulting March 2022.

5. *Research on Privacy Concerns and Data Sharing,* AK Research & Consulting March 2025.

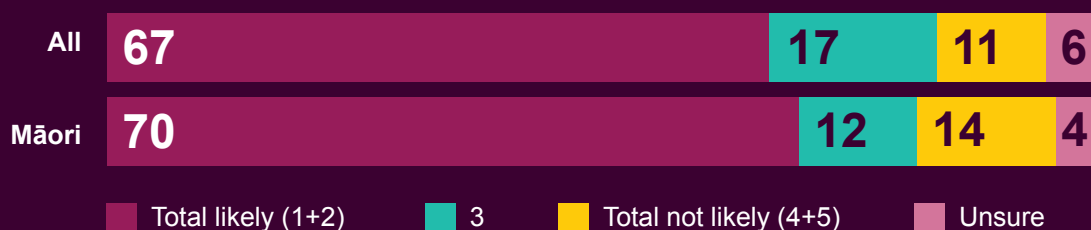
6. *Research on Privacy Concerns and Data Sharing,* AK Research & Consulting April 2024.

## Māori experiences related to privacy

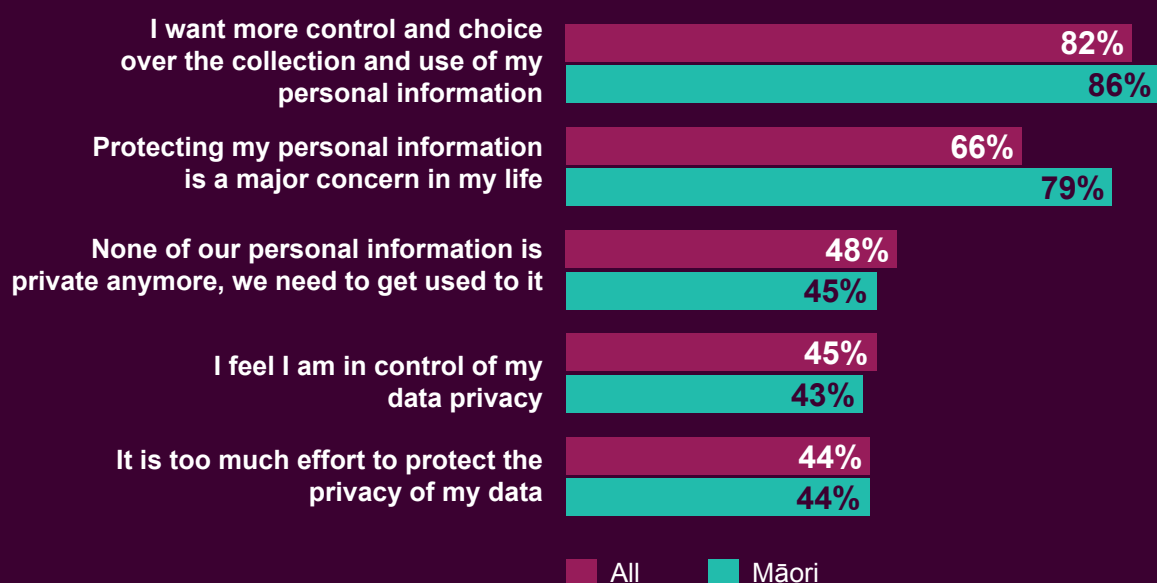
Are you aware that the Privacy Act gives you the right to a copy of any personal information an organisation holds about you? (%)



How likely would you be to consider changing service providers if you heard they had poor privacy and security practices? (%)



Thinking about the privacy of your personal information, to what extent do you agree or disagree with the following? (% total agree)



Source: [Research on Privacy Concerns and Data Sharing, March 2025](#). AK Research & Consulting, prepared for the Privacy Commissioner

## CASE STUDY

### Establishing Te Ranga Tautiaki, our Māori reference panel

*Kotahi te aho ka whati, ki te kāpuia e kore e whati*

*One strand of flax is easy to break, but many strands together will stand strong.*

In December 2024 we established the Māori Reference Panel to provide us with advice and provide insights to ensure more robust thinking and a better knowledge about working within the Treaty of Waitangi, Māori cultural perspectives and tikanga Māori. This includes providing te ao Māori perspectives and thoughts on programmes to enhance the strategic direction of our Office.

The panel also assists us with our engagement activities, by helping us connect with key Māori communities and guiding us in how to better engage with Māori and through making connections.

The Panel met three times in 2024/25, covering topics as broad as the development of the Biometrics Processing Privacy Code, the Inquiry into Foodstuffs North Island trial use of Facial Recognition Technology and our role as a privacy system influencer.

The members of our Māori Reference Panel are leaders who know the heartbeat of their people and communities, and privacy and data experts. The members of our rūpū are:

- Chris Cormack (Kāi Tahu, Kāti Māmoe, Waitaha)
- Tahu Kukutai (Ngāti Tīpā, Ngāti Mahanga, Ngāti Kinohaku, Te Aupōuri)
- Vanessa Clark (Waikato; Ngāti Tīpa, Ngāti Tahinga, Ngāti Āmaru)
- Kura Moeahu QSO (Te Kāhui Maunga, Ngā Ruahine, Te Āti Awa, Ngāti Mutunga, Taranaki-tuturu, Ngāti Tama, Ngāti Toa)
- Māhera Maihi (Ngāpuhi, Ngāti Whātua, Muriwhenua)
- Mercia-Dawn Yates (Te Arawa, Te Aitanga-a-Mahaki, Rongowhakaata, Ngāti Maniapoto).

The Panel is chaired by the Privacy Commissioner, Michael Webster.





## Objective 2:

We will engage and empower people and communities who are more vulnerable to serious privacy harm

Our functions that directly support Objective 2: Communication and Education.

The Act provides New Zealanders with important rights they can use to increase their confidence that their privacy is being protected and to protect themselves from privacy harm. These rights include being informed about why an agency is wanting to collect their personal information and who will receive the information. After collection, the Act then provides New Zealanders with a right to access a copy of their information and to seek a correction should the personal information be incorrect.

Individuals have an important role in ensuring privacy is a core focus for agencies. Agencies will prioritise privacy if their customers and clients challenge them on why and how much personal information is being collected, seek corrections to their personal information or complain if their privacy has been interfered with. New Zealanders are also proactive about letting us know about areas of non-compliance or privacy concerns that they have.

Focusing on outreach and engagement aims to increase understanding of privacy rights and ensure that we provide the right information in an accessible way. Our aim is to target people and communities who are more vulnerable to serious privacy harm, as we believe this will deliver the best improvement in privacy outcomes. We do this through our public enquiries function and our media related activities.

Over the period of 2023–2027 the Statement of Intent outlined our ambition to:

- improve our digital service channels so that they provide people with what they need (including replacing our existing website)
- undertake outreach and engagement activities focused on understanding those parts of society that are more vulnerable to serious privacy harm and working with others to empower them to use their privacy rights.

### The challenges ahead of us

New Zealanders are living in an increasingly complex environment, with new technologies and detailed terms of service documents they are expected to read, understand and accept. This environment emphasises the need for New Zealanders to be aware of their privacy rights but also leads us to notification fatigue and people clicking 'Accept' without engaging.

Our diverse country means there are people and communities who will be more vulnerable to serious privacy harm. This includes demographics such as children, elderly, the disabled community, the rainbow community, Māori and immigrant communities. It can also include people in vulnerable situations, such as children in the Oranga Tamariki system, beneficiaries, victims of crime, inmates, and patients in the health system.



As a small office it is difficult for us to reach all these communities. To maximise our impact, we will be seeking to:

- issue privacy guidance to the education sector, a key objective of which is to empower the privacy understanding of children and young people and their parents/caregivers
- develop and implement an engagement programme focused on educating an identified group of New Zealanders on their privacy rights
- in response to the increasing volumes, reviewing our systems and processes for responding to enquiries.

### Our progress and achievements in 2024/25

Our focus with our digital service channels has been to refresh the presentation and content of the existing website. We have made excellent progress with this refresh this year, as outlined in the case study later in this section. The effect of the refresh is to make the information on our website more accessible and easier to read so that we can better inform New Zealanders of their privacy rights and agencies of their responsibilities.

Over the past 12 months we have also undertaken the following engagement activities. We:

- responded to a total of 6,247 enquiries, with 3,100 of these handled in-house
- applied our ‘fast resolve’ approach to 1,208 privacy complaints that we received, which empowers individuals to exercise their privacy rights and helps agencies understand their obligations under the Act
- received and responded to 164 media enquiries
- received 84 requests for speeches and presentations across the motu, which saw various staff speaking to schools, law firms, not for profit groups and others (in person and online) about doing privacy well
- had over 1,400,000 unique pageviews of our website, an increase of 8% over the prior year.

### Assessing our impact

Indicator	Public awareness of the right to access personal information under the Privacy Act
Baseline (year)	47% (2022) <sup>7</sup>
Desired change	Increase
<b>2024/25 result</b>	<b>53% (2025)</b>
2023/24 result	50%

The public’s awareness of their right to access personal information is an important indicator for the outcome that ‘individuals are more confident that their privacy is protected’. We use this indicator as a proxy for privacy understanding of individuals.

The right to access personal information is a long standing right and was in the Privacy Act 1993. Exercising your right to access personal information then allows you to exercise another of your privacy rights: your right to request that an agency correct your personal information.

We measure this indicator through our privacy survey. Our baseline result of 47% awareness of the access right was a mixed result as it left significant room for improvement. The 2023/2024 result was 50% and the 2024/25 result is 53%. This increase remains small but promising and we are mindful that the increase remains close to the statistical margins of errors for the survey.

7. Privacy concerns and sharing data, Omnibus research commissioned by the Privacy Commissioner. AK Research & Consulting March 2022.

Indicator	Significant improvements made to digital service channels
Baseline (year)	New measure
Desired change	Increase
<b>2024/25 result</b>	<b>Achieved</b>
2023/24 result	Achieved Refer to Function 2 for details

During 2024/25 our focus has been on condensing and improving the presentation and plain language on a range of pages on our website. We developed a new organisational ‘look and feel’ for our Office, created a new front page for our website and reviewed the website to make key information more easily accessible. More information on what we achieved is available in the case study later in this section.



THE TOP FIVE FREQUENTLY  
ASKED QUESTIONS WERE  
ACCESSED NEARLY

**35,000**

TIMES IN 2024/25

Indicator	Respond to all public enquiries within five working days
Baseline (year)	99% (2021/22) <sup>8</sup>
Desired change	Maintain
<b>2024/25 result</b>	<b>90%</b>
2023/24 result	96%

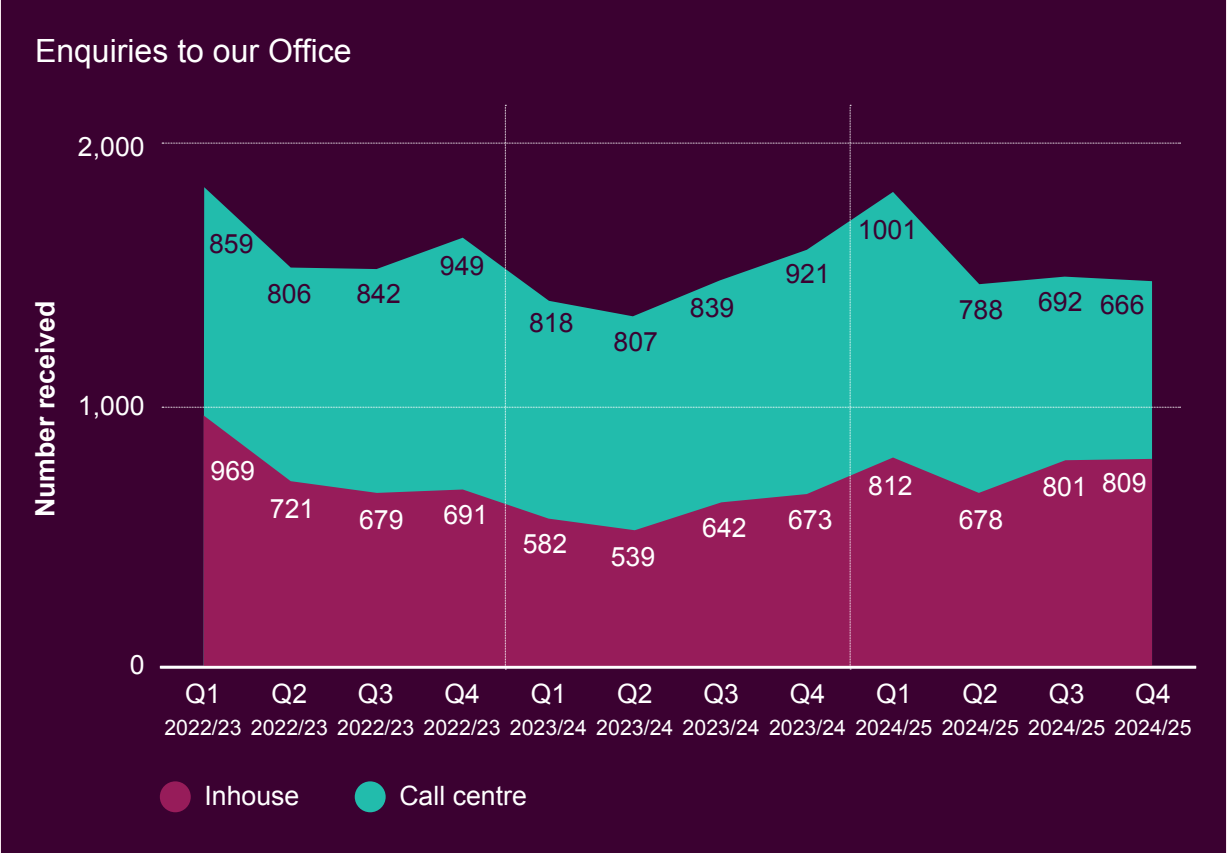
We seek to promptly respond to public enquiries because informed individuals can better exercise their privacy rights and protect themselves. Our baseline results for this indicator is excellent, with 99% public enquiries responded to within five working days in 2021/22 and 2022/23.

The timeliness of our responses to public enquiries has been decreasing as the volumes of enquiries, privacy complaints and breach notifications have increased significantly. Our result for this year is 90% of public enquiries responded within five working days.

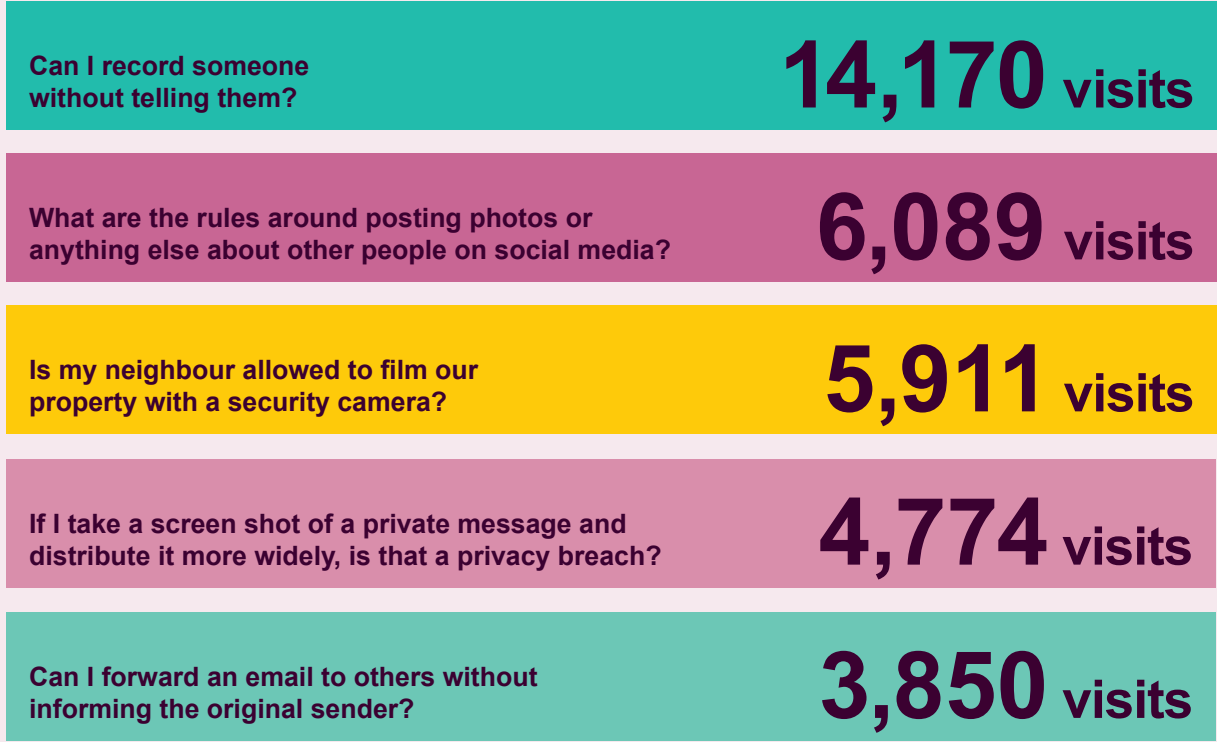
Our enquiry function draws upon and supplements the information on our website, including our AskUs database of common privacy questions and answers. AskUs has high usage by the public, with the top five frequently asked questions accessed nearly 35,000 times in 2024/25.

8. The figure reported in the 2022 Annual Report of 94% was against a measure of responding within 2 working days. The figure shown here has been calculated at 5 working days for comparative purposes.

Data relating to our enquiries and AskUs functions



The top five questions people want to know about our 'AskUs' page:



## CASE STUDY

### Improving privacy.org.nz

Our Office's website is the portal for notifying privacy breaches for agencies, and it is a key tool for how New Zealanders learn and complain about their privacy rights. The website also has an education role about privacy through case notes, decision notes, and our e-learning modules.

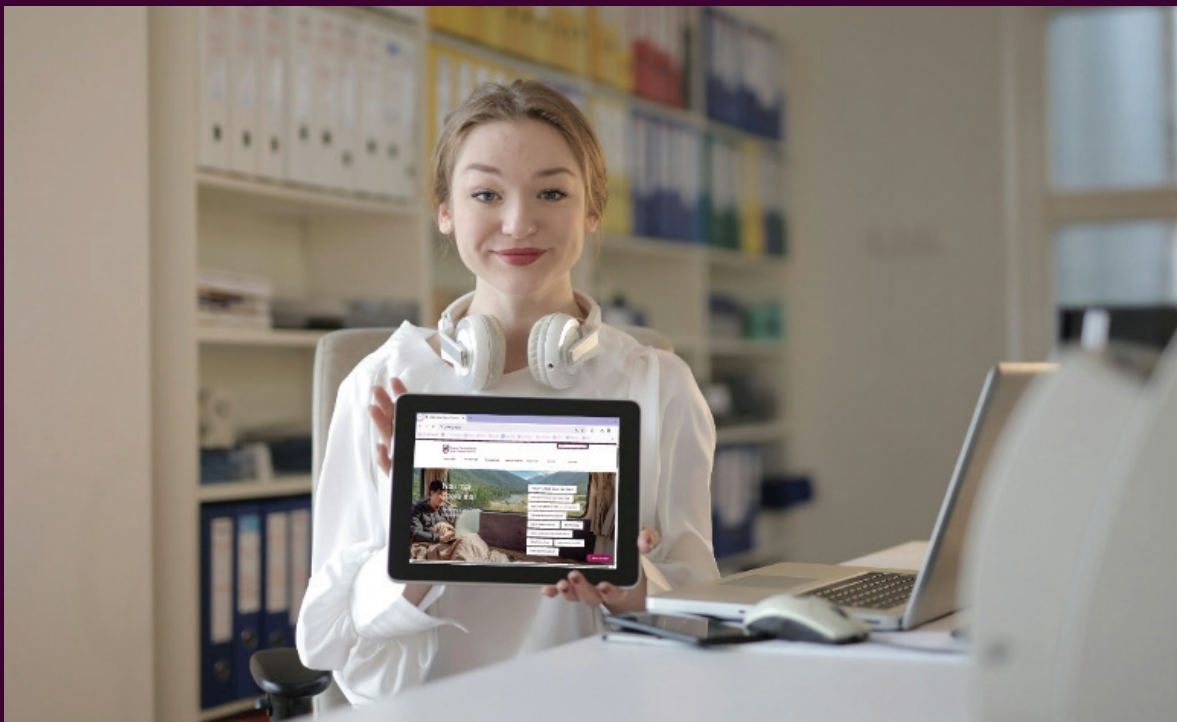
Privacy.org.nz is a website full of excellent content where publishing has been promoted for several years instead of active maintenance. The result was a website with a lot of historical content where contemporary information was hard to find.

Our website redevelopment project began this year and is ongoing. Changes include:

- a contemporary homepage that lets us more easily showcase short-term content through homepage banner tiles and story features

- the development of a new menu that groups content together, and logically so it's becoming easier to find
- moving the website into a plain language framework
- archiving out of date content
- using images to demonstrate that privacy is about people
- working towards becoming more accessible.

These changes have created a website where New Zealanders can increasingly find answers to their privacy questions, whether they're individuals or agencies. The work, which is being done in-house will continue until the 2026/7 financial year.





### Objective 3:

We will set clear expectations to provide agencies with greater certainty about their responsibilities

Our functions that directly support Objective 3: Policy and Advocacy.

One way the Act improves privacy outcomes is through establishing for agencies obligations and safeguards for collecting, using and sharing personal information. Examples of these requirements include notifying individuals what personal information the agency is seeking to collect, a requirement to store the personal information securely and only using or disclosing the personal information for specific reasons.

As the regulator, we need to set clear expectations so that agencies can understand what the Act requirements are in order to meet them. We will accomplish this through issuing guidance on implementing the Act, maintaining up to date codes of practice and having useful tools for agencies to use (such as our e-learning modules).

Over the period of 2023–2027 the Statement of Intent outlined our ambition to:

- provide agencies with greater certainty through setting specific, strong, and clear expectations, focusing on areas where there are the most significant power imbalances between individuals and agencies and/or sensitive information is involved
- support agency understanding and capability by supporting the development of, and engaging with, the privacy profession (both in-house privacy professionals and privacy advisors)
- ensure that codes of practice issued under the Act and our guidance, advice and education material are fit for purpose
- expect Government and businesses to demonstrate that their privacy related activities are necessary and proportional.

#### The challenges ahead of us

Managing privacy well requires that agencies consider their circumstances; it is not a tick box exercise. In addition, our broad scope extends to nearly the entire public, private and not-for-profit sectors. These factors lead to a large demand for certainty from us as the regulator.

This desire for certainty is also driven through the development and adoption of new technologies. While the Act takes an adaptable principles-based approach to regulation and is best viewed as a 'how to' (rather than a 'do not do'), it further increases the demand for us to provide clear and timely guidance.



Looking forward, we will continue our focus on producing excellent privacy advice on the government’s legislative programme and guidance for agencies. We will also be reviewing Codes of Practice to accommodate the new indirect notification principle being established in the Privacy Amendment Bill and amending the Telecommunications Information Privacy Code to support the provision of location information in emergencies.

**Our progress and achievements in 2024/25**

We have made excellent progress on this objective this year.

We committed a large amount of resource to setting clear expectations for biometrics technologies, such as facial recognition. There were two main projects in this space:

- The Inquiry into Foodstuffs North Island trial use of FRT, which was completed in May 2025 and found that the trial use of FRT complied with the Act. Our Inquiry findings received a high level of attention and have clearly communicated our expectations as regulator for how agencies can implement FRT systems in a privacy protective manner.
- The development of the Biometric Processing Privacy Code which was released in August 2025 will create more specific rules for agencies using biometric technologies. These rules will help make sure agencies implementing biometric technologies do it safely and in a way that is proportionate. To assist implementing the Code, a comprehensive suite of guidance was also developed and consulted on in 2024/25.

Throughout the year we provided advice to government agencies, Cabinet and Parliament on the privacy implications of the Government’s legislative programme. A key aspect of our advice is to consider whether proposed legislative amendments are necessary and that the impacts on personal privacy are justified and proportionate. Over the year we provided privacy advice to dozens of agencies and made 12 submissions to Parliamentary Select Committees on the privacy implications of specific legislative bills.

Parliament has been progressing the Privacy Amendment Bill, which establishes in the Act a new indirect notification requirement for agencies. Currently due to come into force on 1 May 2026, we have developed guidance that will assist agencies in meeting this new Act requirement.

We provide a range of resources and tools to agencies to help them build their understanding and succeed at managing privacy well. This year we also issued a range of new guidance, including tenancy guidance for landlords and tenants, complaint handling guidance, and guidance on the use of third-party providers.

Every year in May we run ‘Privacy Week’ during which we host a variety of events and issue materials that promote good privacy practice. This year our Privacy Week theme was ‘Privacy on Purpose’, where we had 21 presentations watched by over 8,500 people – an increase of over 60% from 2023/24. The most popular topics included ‘AI and privacy: The Foundation You Can’t Ignore’ and ‘Back to the Future: What have we learned from two years of popular AI tools?’

**Assessing our impact**

Indicator	Awareness of Privacy Act requirements
Baseline (year)	New measure
Desired change	Increase
2024/25 result	See next subsection
2023/24 result	See Annual Report 2023/24

The broad scope of the privacy system makes it extremely difficult to gauge the level of awareness that agencies have of Act requirements. Many agencies have a low level of understanding of the Act and those that we do interact with are often not aware of their full obligations under the Act.

Last year, to estimate the awareness of requirements under the Act, we leveraged the results of surveys undertaken by other agencies. We took this approach as our limited resources mean that we cannot engage with a representative sample of agencies in New Zealand to build a comprehensive picture of privacy understanding across the economy.



During this year we sought to improve on last year's approach by including a few key privacy questions inserted into surveys that other agencies were commissioning. These questions would relate to agencies having a Privacy Officer (a statutory requirement), privacy training and policies and procedures in place for privacy breaches.

We had very limited success with this approach and are reviewing our approach for 2025/26. We contacted a variety of agencies who had conducted surveys of specific sectors in the past, but had very little uptake. The case study later in this section provides information from a small survey that we conducted through the Institute of Directors.

Indicator	Undertake two projects per year relevant to setting privacy standards, expectations, or guidance in the privacy system
Baseline (year)	New measure
Desired change	Maintain
<b>2024/25 result</b>	<b>Achieved</b>
2023/24 result	Achieved

This indicator is an important part of ensuring that we continue to set clear expectations for agencies in the privacy system. Significant projects related to setting privacy standards, expectations or guidance this year included:

- completing the Inquiry into Foodstuffs North Island trial use of Facial Recognition Technology
- completing the development of the Biometric Processing Privacy Code
- developing guidance to help implement the new indirect notification principle that will be introduced by the Privacy Amendment Bill.

Indicator	Percentage of externally reviewed policy files that are rated as 3.5 out of 5 or better for quality
Baseline (year)	95% (2022)
Desired change	Maintain
<b>2024/25 result</b>	<b>93%</b>
2023/24 result	100%

Ensuring that we undertake high quality work is an important aspect of ensuring that the work we are doing is of a high quality and so more likely to set clear expectations for agencies. This annual review is undertaken by an external consulting firm and assesses a random sample of the work undertaken by our Policy team. We are very pleased with the result of the review this year, which was 93%.

### Data relating to agency privacy understanding – insights from Directors

The Institute of Directors conducts surveys of their members that help provide an insight into the privacy understanding (and practices) of agencies.

In 2024, the Institute of Directors surveyed 1,000 of their members and found that 57% of their respondents said they discussed privacy practices and risks (an increase of 2% compared to 2023) and that 55% received comprehensive data breach/risk reports (an increase of 1% compared to 2023).

In 2025, we worked with the Institute of Directors to run a survey to gauge the privacy practices of agencies they were directors of.

While small, with 53 respondents, the results of this survey were as follows:

- 66% of Directors said that either all or some of the agencies they were directors of had a Privacy Officer.
- 64% of Directors said that either all or some of the agencies they were directors of made privacy training available to staff.
- 92% of Directors said that either all or some of the agencies they were a director of had policies and procedure in place to help manage privacy breaches.

These results show there is a significant opportunity for us to promote privacy amongst directors as a part of their duties.

## CASE STUDY

### Inquiry into Foodstuffs North Island trial use of Facial Recognition Technology

Between February to September 2024, Foodstuffs North Island ran a trial of Facial Recognition Technology (FRT) in 25 of their New World and PAK'nSAVE branded supermarkets. During this trial, FRT systems scanned over 225 million faces (including multiple scans of the same person), with 99.999% of images deleted within one minute. The systems raised 1,742 alerts of which 1,208 were later confirmed as matches by staff.

We ran an Inquiry alongside this trial use of FRT and completed it in May 2025. Our Inquiry sought to understand the privacy impacts of the trial, compliance with the Act, and whether the use of FRT was effective in making a difference to the level of serious retail crime. The Commissioner's inquiry function was used to assess whether the live FRT trial infringed on the privacy of individuals. The potential privacy concerns included the unnecessary or unfair collection of people's personal information, risks of misidentification and bias.

The Inquiry found that the trial use of FRT complied with the Act, based on how the FRT model had been designed and deployed. We found that while the level of inherent privacy intrusion was high (as every visitor's face is collected), the privacy safeguards in the trial reduced the level of intrusion to an acceptable level. We found the trial was effective in addressing its purposes of reducing repeat serious harmful behaviour in the recent past, including physical and verbal assault and higher value theft.

Our report recommended several improvements to Foodstuffs North Island. We recommended that documented processes and system settings should be updated to reflect what happens in practice, an ongoing review of effectiveness should occur and monitoring and review to evaluate the impact of skin tone on identification accuracy and store response.

Our Inquiry sets clear expectations for all agencies considering FRT systems in the following areas:

1. Careful thought before deploying FRT
2. Setting up and maintaining the watchlist
3. Installing and maintaining the wider FRT operating system
4. Information for customers about FRT and access/correction of information
5. Alerts
6. Decisions about whether and how to intervene
7. Security of your FRT systems and information
8. Managing complaints and access or correction requests
9. Review and monitoring





## **Objective 4:**

**We will promptly use our full range of investigation and compliance powers to hold agencies accountable for serious privacy harm**

**Our functions that directly support Objective 4: Compliance and Enforcement, Investigations and Dispute Resolution.**

Our approach to compliance is that we encourage and support agencies in meeting their privacy requirements and that we act to hold agencies to account where necessary to address non-compliance. Our Compliance and Regulatory Action Framework sets out our escalation approach to encourage agencies to meet their requirements.

We promote strong privacy outcomes by using our full range of investigation and compliance powers when it is warranted. We issue compliance letters setting out our expectations with agencies about their privacy practices, issue Compliance Notices requiring agencies to alter their practices and publicly name agencies we find to be in breach of the Act in line with our Naming Policy. The use of these tools ensures the sector understands how we will respond when needed.

Over the period of 2023–2027 the Statement of Intent outlined our ambition to:

- have our compliance activities prioritise systemic privacy issues relating to those parts of society that are more vulnerable to serious privacy harm, especially when those issues stop individuals from exercising their privacy rights
- promptly triage and investigate privacy complaints and breach notifications, while accounting for cultural needs and recommending redress where possible
- inform our work with insights from identified privacy system risks, international experiences and our own data.

### **The challenges ahead of us**

The key challenge facing us is the increasing volumes and complexity of privacy breaches and complaints that we are receiving. These factors place increasing pressure on our staff and also the accomplishment of key performance indicators.

The demands on our functions means that we constantly prioritise the use of our investigation and compliance powers. This demand arises from the broad scope of the privacy system, where privacy breaches and complaints can occur anywhere and be very different in cause, impact, sector and size.

The lack of penalties within the Act provides agencies with few financial incentives to take privacy seriously. This situation means that many agencies have a low level of understanding of the Act.

### **Our progress and achievements in 2024/25**

Continuing to strengthen our Compliance and Enforcement function is a key area of strategic focus for us. A key achievement for our compliance function includes triaging and reviewing 1,093 privacy breach notifications and then following up on privacy breaches that are likely to cause serious harm. Our activities in this area encourage agencies to swiftly address privacy breaches and to build their capability to help avoid future privacy breaches.

During this year we also publicly issued a Compliance Notice to Oranga Tamariki on their failure to comply with Act requirements relating to storage and security and disclosing personal information. This action was taken as Oranga Tamariki needed to take additional steps to improve their privacy practices after a series of privacy breaches that caused serious harm to whānau and tamariki. Particular areas of improvement related to staff skills and strengthening the information access settings, oversight of service providers and the reporting of privacy incidents.

During 2024/25 our Investigations and Dispute Resolution function experienced record high levels of privacy complaints with 1,598 privacy complaints received from individuals. We took a ‘fast resolve’ approach to 1,208 of these complaints, for example through encouraging the individual to first approach the relevant agency with their complaint. This approach promotes the best outcomes for complainants within a quick timeframe.

Where we investigate a privacy complaint, we have a strong dispute resolution mandate and negotiated financial settlements for 6.5% of the privacy complaints. Investigating and resolving privacy complaints is very important to complainants as it provides them with redress and helps restore their confidence that their privacy is protected.



**Investigating and resolving privacy complaints is very important to complainants as it provides them with redress and helps restore their confidence that their privacy is protected.**

### Assessing our impact

Indicator	Percentage of serious privacy breaches notified to our Office within 72 hours
Baseline (year)	61% (2022/23)
Desired change	Increase
<b>2024/25 result</b>	<b>71%</b>
2023/24 result	60%

We assess our impact in this area through the promptness which serious privacy breaches are notified to our Office. It is a statutory requirement for agencies to notify the Privacy Commissioner as soon as practical of any privacy breach where it is reasonable to believe an individual could suffer serious harm. We have issued clear guidance that we expect these notifications to be provided to us within 72 hours.

In 2023/24 we had 60% of serious privacy breaches notified to our Office within 72 hours and we are aiming to improve this percentage. This year the percentage of serious privacy breaches notified to us within 72 hours increased to 71%. The increase in this measure this year was in part due to a series of similar breaches being notified promptly by one particular sector.

Indicator	Notified privacy breaches that are likely to cause serious harm, are followed up with the notifying agency within 10 working days of receipt
Baseline (year)	New measure
Desired change	Maintain
<b>2024/25 result</b>	<b>95%</b>
2023/24 result	85%

We follow up with agencies who have notified us of serious privacy breaches to help ensure that agencies are responding well and mitigating the harm to affected individuals. Our target for this measure in 2023/24 was a 100% follow up rate, however this has proven unrealistically high and resource intensive. We are very happy with our result of 95% for 2024/25. We will be seeking to maintain this percentage going forward.

Indicator	The percentage of complaints closed during the year that were less than six months old at closure
Baseline (year)	84% (2022/23)
Desired change	Maintain
2024/25 result	88%
2023/24 result	75% <sup>9</sup>

We are seeking to maintain timeliness in resolving privacy complaints so that agencies consider that we act promptly when serious privacy harms occur. For this measure we also include our ‘fast resolve’ complaints.

Note that during this year, some discrepancies were identified in the way data for ‘fast resolve’ complaints were being captured. These have been rectified, appropriate system amendments made and, as a result, the comparatives have been updated

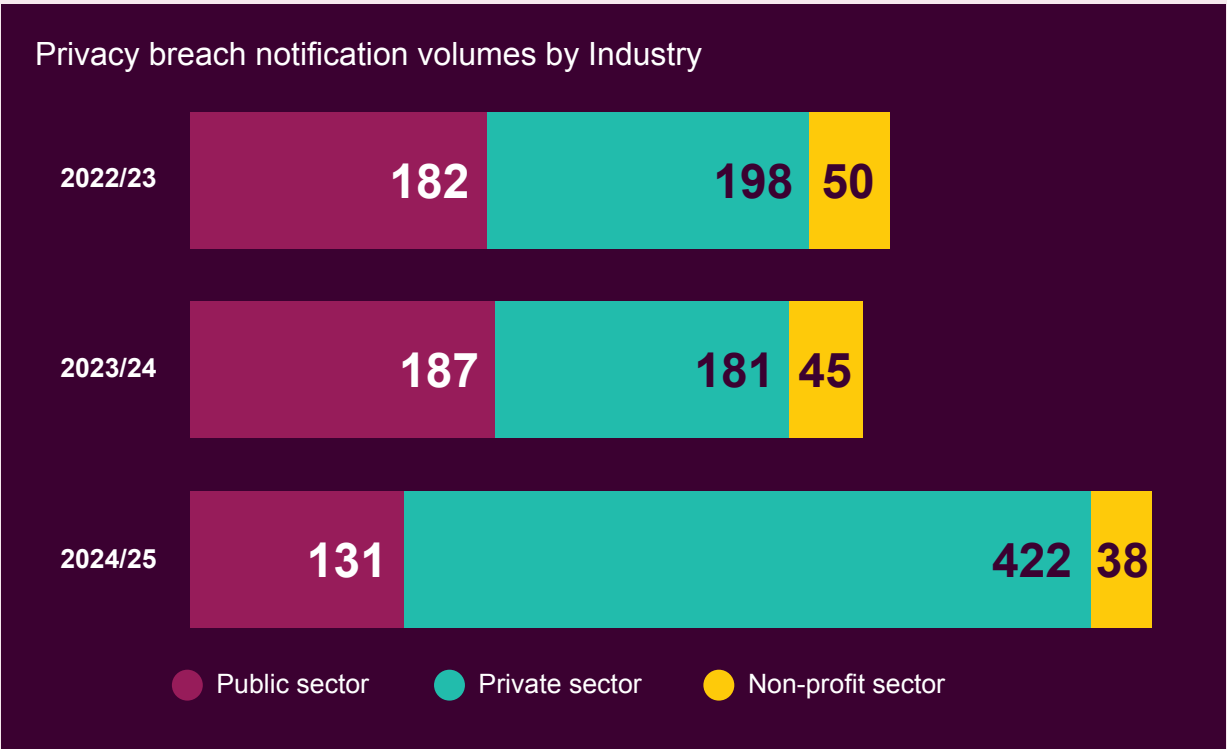
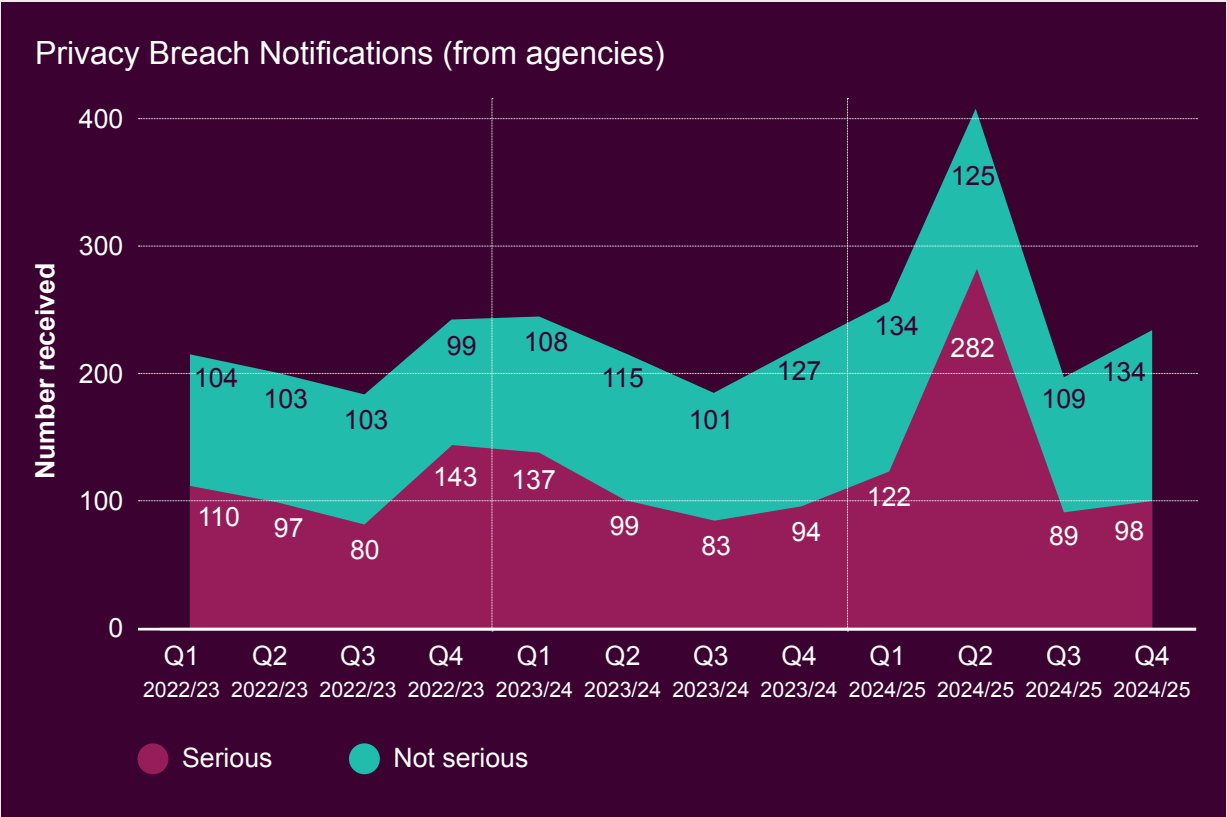
The 2024/25 result of 88% reflects a good result during a period of high and increasing volumes. However, we are mindful that if a privacy complaint requires a complicated or comprehensive investigation the high volumes and limited resourcing we have means that the wait time for an investigator can be up to six months.

Indicator	The percentage of externally reviewed compliance investigations that are rated as 3.5 out of 5 or better for quality
Baseline (year)	New measure
Desired change	Maintain
2024/25 result	100%
2023/24 result	100%

We want our Compliance and Enforcement investigations to be of high quality to ensure that our interventions are correct and effective. The result of our external quality review of our compliance investigations and compliance notices continues to be extremely pleasing and we will be seeking to maintain this quality going forward.

9. The 2023/24 result has been restated to reflect changes in the data captured. In the prior year’s annual report, the result for this indicator was reported as 69%

Data relating to our compliance activities





Data relating to our compliance activities



## CASE STUDY

### Restoring the mana of teachers through complaint investigation and conciliation

We received privacy complaints from three teachers relating to their school accessing private social media messages they had sent to each other.

The complaints arose after one of the teachers returned her work laptop to school when they stopped working at the school. When a school administrator checked the laptop for later use, they found the laptop was still logged into the teacher's personal Google and Facebook accounts. Facebook Messenger messages between the three teachers were accessed and screenshots provided to the Principal, who raised the issue with the teachers who were still employed by the school.

The teachers complained to the school but were told that the information had been accessed in accordance with its duty as an employer and that no apology was necessary.

The three teachers then made privacy complaints to our Office. We notified the school that we were commencing an investigation into a possible privacy breach relating to the collection of personal information. The school's initial response was that as the collection of personal information was unsolicited, they were not required to comply with the collection principles of the Act.

After investigating this situation and discussing it with both sides, we set out our preliminary view that the school had breached the collection principles of the Act and interfered with all three teachers' privacy. Our view was that it was not necessary for the school to collect the information (as the teacher had left the school) and they had intruded unreasonably into the personal affairs of the teachers (as unrelated personal messages were also accessed).

The school accepted our view and agreed to an in-person conciliation that we facilitated. The conciliation was very positive, with the school wanting a process that restored the teachers' mana. Each of the teachers was able to fully explain the impacts of the breaches on them. We assisted the parties to reach a suitable resolution which was tailored to each of the complainants.



# Office and functions

Te Tari me āna mahi



## Independence and other interests

The Privacy Commissioner has wide ranging functions. The Commissioner must have regard to the information privacy principles in the Privacy Act and the privacy interests of individuals alongside other important human rights and social interests.

Relevant rights and social interests include the desirability of a free flow of information and government and business being able to achieve their objectives in an efficient way. The Commissioner must take account of New Zealand's international obligations and consider any general international guidelines that are relevant to improved protection of individual privacy. The Commissioner must also take account of cultural perspectives on privacy.

The Privacy Commissioner is independent of the Executive. This means the Commissioner is free from influence by the Executive when investigating complaints, including those against Ministers or their departments. Independence is also important when examining the privacy implications of proposed new laws and information sharing programmes.



**Relevant rights and social interests include the desirability of a free flow of information and government and business being able to achieve their objectives in an efficient way.**

## Reporting

The Privacy Commissioner reports to Parliament through the Minister of Justice and is accountable as an independent Crown entity under the Crown Entities Act 2004.

## Staff

We employ staff in our Auckland and Wellington offices. During the year to 30 June 2025, the senior leadership team was made up as follows:

The Deputy Privacy Commissioner: responsible for 4 teams – Investigations and Dispute Resolution, Compliance and Enforcement, Capability and Guidance and Policy

The General Manager: responsible for Support Services and Finance and Performance, Strategy Insights and International, Communications and Engagement and our Pou Ārahi. We employ administrative support staff in both offices.

The General Counsel: legal counsel to the Privacy Commissioner, manages litigation, and gives advice around investigations and law reforms.

## Statutory Remuneration Disclosures

The Office of the Privacy Commissioner is a Crown Entity and is required to disclose certain remuneration information in its annual reports. The disclosures required are set out in Section 152 of the Crown Entities Act 2004 (CEA).

## Employees Remuneration

The number of employees receiving total remuneration of \$100,000 or more per annum is disclosed below in \$10,000 bands. This table does not include the Commissioner as he is disclosed separately below.

Total remuneration and benefits	Number of employees	
	Actual 2025	Actual 2024
\$100,000 – \$109,999	6	3
\$110,000 – \$119,999	4	1
\$120,000 – \$129,999	1	1
\$130,000 – \$139,999	3	1
\$140,000 – \$149,999	1	1
\$150,000 – \$159,999	-	3
\$160,000 – \$169,999	1	1
\$170,000 – \$179,999	1	2
\$180,000 – \$189,999	-	-
\$190,000 – \$199,999	1	-
\$200,000 – \$209,999	-	2
\$210,000 – \$219,999	2	-
\$340,000 – \$349,999	-	1
\$360,000 – \$369,000	1	-

## Commissioner's total remuneration

In accordance with the disclosure requirements of section 152(1)(a) of the CEA, the total remuneration, as set independently by the Remuneration Authority, includes all benefits paid during the period 1 July 2024 to 30 June 2025.

Name	Position	Amount 2025	Amount 2024
Michael Webster	Privacy Commissioner	\$421,149	414,288

## Severance payments

Severance payments relate to the termination of employment whether monetary in nature or otherwise. These payments are additional to any final payment of salary, holiday pay or superannuation contributions. For the year ended 30 June 2025, there was no severance payment made (30 June 2024: \$27,465).

## Indemnity and Insurance disclosures

The Privacy Commissioner's insurance policy covers public liability of \$10million and professional indemnity of \$1million.

## EEO Profile

Our human resource policies and programmes are aligned to and consistent with our EEO Policy, as outlined in our Statement of Intent 2023–2027. In addition, we have policies in place to address employee professional development needs, harassment prevention, as well as health, safety and employee wellbeing.

As a member of Te Uru Tāngata Centre for Workplace Inclusion (previously named Diversity Works New Zealand), we seek to follow good practice in key areas such as recruitment and career development to ensure we attract and retain the talent we need to

deliver on our ambitious work programmes. We have support also from our Health, Safety and Wellbeing Committee, made up of staff across the organisation. This group is actively involved in developing new initiatives to respond to areas of need with a strong focus on employee wellbeing and resilience.

During the year we updated our Kia Toipoto Action Plan to address pay inequities – particularly for Māori, Pacific, other ethnic pay groups, and members of the Rainbow and disability communities. This supports our commitment of ensuring fair workplace practices and delivering a diverse and inclusive workplace.

## Workplace FTE profile – as at 30 June 2025

Role	Number of staff			Total
	Full-time	Part-time	Fixed-term	
Commissioner	1			1
Deputy Commissioner	1			1
Senior managers	2			2
Team and unit managers	7	3		10
Investigations and Dispute Resolution	6	2	1	9
Administrative support	4	3		7
Policy	4	1		5
Compliance and Enforcement	6			6
Capability and Guidance	1	1		2
Strategy, Insights and Communications	2	1		3
Legal	1	1		2
<b>Total</b>	<b>35</b>	<b>12</b>	<b>1</b>	<b>48</b>

The figures above don't include secondees and contractors

# Finance and performance



Pūrongo whakahaere pūtea  
me ngā tutukitanga





# Statement of performance

The Justice Sector has an aspirational outcome that all New Zealanders should expect to live in a safe and just society. We support this aspiration as a Justice Sector Crown entity.

While the Office of the Privacy Commissioner is an independent Crown entity and strongly maintains such independence, our Statement of Intent and Statement of Performance Expectations set out a work programme that complements this aspiration and government priorities as a whole.

Our Statement of Intent 2023–2027 identifies four high level objectives to support our mission to be an “effective modern privacy regulator”. The “Strategic objectives progress” section of this Annual Report provides specific evidence on how the Office has performed against each of these objectives during the year.

In order to achieve the high-level objectives, the Office also identified three strategic priorities for the 2024/25 year as outlined in our Statement of Performance Expectations for the year ended 30 June 2025. These priorities are:

- continuing to build our strengthened Compliance and Enforcement function
- delivering on our regulatory stewardship responsibilities
- ensuring the Privacy Act is fit-for-purpose in the digital age.

A summary of the key work undertaken within each of these areas is also highlighted in the section noted above.

To support the delivery of our strategic focus, we have determined five output class areas (Functions) that contribute to the overall outcome. These are consistent with the previous year and we report our progress against these Functions in this section.

# PBE FRS 48 Service Performance Reporting

PBE FRS 48 is the relevant reporting standard and establishes generally accepted accounting practice and high-level requirements for reporting on service performance. This standard has been applied when collating and reporting information for the Service Performance measures for the year ended 30 June 2025.

As noted above, the Statement of Intent covering the period 1 July 2023 to 30 June 2027 and the Statement of Performance Expectations for the year to 30 June 2025 each set out the longer-term strategy of the Office as well as the specific priorities set for the year to 30 June 2025. The three priorities identified for the 2025 year, were a continuation of areas identified in the 2024 year following a detailed analysis of themes from business intelligence sources as well as internal office discussions. During the year, the Office has successfully developed the Biometrics Processing Privacy Code and completed the inquiry into Foodstuffs North Island trial use of Facial Recognition Technology.

## How the measures were selected

The performance measures have remained consistent with those included in the prior year Annual Report. There have been some changes to rewording of measures within Communications and Engagement, and Compliance and Enforcement functions to better reflect the Office's current environment and fiscal savings.

The final proposed suite of measures is subject to a thorough review process, both internally and through the Estimates of Appropriation process with the Ministry of Justice to ensure consistency with Estimates set out in the Vote Justice document. The Office considers feedback that it receives and makes changes it thinks are necessary or would improve overall reporting.

## Judgements and measurements

A certain amount of judgement is required to be made when setting the targets against the measures. This judgement considers both previous performance as well as future expectations. Targets have been reviewed to focus on data capturing mechanisms and qualitative characteristics.

As part of the annual review of measures, the Office also considers whether systems for capturing and recording the data are in place. Most of the data required for reporting is captured within the Office's document management system (see the Statement of Performance Expectations which sets out which measures rely on this data) and analysis is undertaken throughout the year, and at year-end, to ensure that the information is fit for purpose. No changes were required to be made to any internal systems as part of the reporting in the year to 30 June 2025. Despite this, amendment has been made in the methodology used to capture data relating to fast resolve complaints and breaches. Refer to the affected measures in the following section for more information. Performance against three of the measures is based on an external assessment. Where this is the case, further information regarding judgements has been provided in the reporting that follows.

# Statement specifying comprehensive income

The Privacy Commissioner agreed the following financial targets with the Minister at the beginning of the year:

**Specified comprehensive income**

	Target \$000	Achievement \$000
Revenue		
Crown revenue	7,640	7,640
Other revenue	146	195
<b>Total income</b>	<b>7,786</b>	<b>7,835</b>

The appropriation received by the Privacy Commissioner equals the government's actual expenses incurred in relation to the appropriations, which is a required disclosure of the Public Finance Act.

The operating grant is received as part of the Non-Departmental Output Expenses – Services from the Privacy Commissioner within Vote Justice. This appropriation is limited to the provision of services concerning privacy issues relating to the collection and disclosure of personal information and the privacy of individuals.

The amount received by the Privacy Commissioner equates to 2% of the total Vote Justice Non-Departmental Output Expenses Appropriation for 2024/25. The total expenses in the year are \$8,087k as set out in the cost of service statement below.

# Cost of service statement

for the year ended 30 June 2025

As set out in the 2024/25 Statement of Performance Expectations, the Privacy Commissioner committed to provide five functions. The split of funds across these five functions is set out below:

	Actual 2025 \$000	Budget 2025 \$000	Actual 2024 \$000
<b>FUNCTION 1: Strategy and insights</b>			
<b>Resources employed</b>			
Revenue	944	1,005	1,117
Expenditure	989	1,113	1,130
<b>Net surplus/(deficit)</b>	<b>(45)</b>	<b>(108)</b>	<b>(13)</b>
<b>FUNCTION 2: Communication and Education</b>			
<b>Resources employed</b>			
Expenditure	1,313	1,432	1,516
Net surplus/(deficit)	1,317	1,522	1,564
<b>Net Surplus/(Deficit)</b>	<b>(4)</b>	<b>(90)</b>	<b>(48)</b>
<b>FUNCTION 3: Compliance and Enforcement</b>			
<b>Resources employed</b>			
Revenue	1,722	1,648	1,791
Expenditure	1,803	1,823	1,812
<b>Net Surplus/(Deficit)</b>	<b>(81)</b>	<b>(175)</b>	<b>(21)</b>
<b>FUNCTION 4: Policy and Advocacy</b>			
<b>Resources employed</b>			
Revenue	1,780	1,938	2,113
Expenditure	1,804	2,081	2,137
<b>Net Surplus/(Deficit)</b>	<b>(24)</b>	<b>(143)</b>	<b>(24)</b>

	Actual 2025 \$000	Budget 2025 \$000	Actual 2024 \$000
<b>PRIMARY ACTIVITY 5: Investigation and dispute resolution</b>			
<b>Resources employed</b>			
Revenue	2,075	1,763	1,900
Expenditure	2,174	1,950	1,950
<b>Net Surplus/(Deficit)</b>	<b>(99)</b>	<b>(187)</b>	<b>(50)</b>
<b>TOTALS</b>			
<b>Resources Employed</b>			
Revenue	7,835	7,786	8,437
Expenditure	8,087	8,489	8,593
<b>Net surplus/(deficit)</b>	<b>(252)</b>	<b>(703)</b>	<b>(156)</b>

The following tables sets out the assessment of our performance against the targets set out in the Statement of Performance Expectations. They also reflect the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation. The following grading system has been used:

Criteria	Rating
On target or better	Achieved
< 10% away from target	Substantially achieved
>10% away from target	Not achieved

# Performance against statements of service performance

for the year ended 30 June 2025

## Function 1: Strategy and Insights

### Activity areas of focus

Promoting better prioritisation and decision making through analysis of enquiries, complaints, privacy breaches and other information we receive. We develop and maintain an understanding of the impact of technological developments on privacy. We monitor the success of our strategies and initiatives.

### Output Measures

Measure	Estimate	Achieved 2024/25	Achieved 2023/24
Conduct 2 assessments a year to gauge the privacy maturity or attitudes of agencies or individuals.	2	<b>Achieved</b> During the year we undertook our 2025 survey of New Zealanders covering privacy concerns and data sharing. We also approached a range of agencies who conduct surveys of specific sectors to see if we could include key questions relating to gauging the privacy understanding of agencies. We then undertook a short survey through the Institute of Directors asking these questions.	<b>Achieved</b> During the year we undertook our biennial survey of New Zealanders covering privacy concerns and data sharing. We have also undertaken an assessment of surveys performed by other agencies, conducted in the year, relating to privacy.

## Function 2: Communications and Education

### Activity areas of focus

Informing people about their privacy rights. Promoting privacy understanding and competence, using media, opinion writing, events and conferences, and stakeholder engagement. Producing material and resources to inform, guide and educate.

### Output Measures

Measure	Estimate	Achieved 2024/25	Achieved 2023/24
Education module completions as a percentage of education module registrations in the year.	75%	<b>Achieved – 82%</b>	<b>Achieved – 84%</b>
Respond to all public enquiries within 5 working days.	95%	<b>Substantially achieved – 90%</b>	<b>Achieved – 96%</b>
Content improvements made to digital service channels. <sup>10</sup>	Achieved	<b>Achieved</b> During 2024/25 our focus has been on condensing and improving the presentation and plain language on a range of pages on our website. We developed a new organisational ‘look and feel’ for OPC and front page for our website, to make key information more easily findable.	<b>Achieved</b> Ongoing revision and development of our web content to ensure clarity and accessibility. Further work to be undertaken in the 2024/25 year.

10. The wording for this measure has been amended from prior year. The previous wording was "Significant improvements made to digital service channels". No change is required to be made on prior year result due to the amended wording.



## Function 3: Compliance and Enforcement

### Activity areas of focus

Identifying and assessing systematic issues, using the right tools to get the best privacy outcomes for New Zealanders, including enforcing the Codes, managing privacy breach responses, prosecution, monitoring of compliance, and enforcement of policy work to ensure compliance.

### Output Measures

Measure	Estimate	Achieved 2024/25	Achieved 2023/24
Notified privacy breaches that are likely to cause serious harm, are followed up with the notifying agency within 10 working days of risk assessment. <sup>11</sup>	85%	<b>Achieved – 95%</b>	<b>Achieved – 85%</b>
The percentage of externally reviewed compliance investigations that are rated as 3.5 out of 5 or better for quality. <sup>12</sup>	85%	<b>Achieved – 100%</b> The review was undertaken by an external consulting firm. The result is based on a review of compliance notices and compliance investigations. <sup>13</sup>	<b>Achieved – 100%</b>
Incoming compliance issues are risk assessed on allocation to determine the appropriate response activity. <sup>14</sup>	90%	<b>Achieved – 99%</b>	<b>Achieved – 98%</b>

11. The wording for this measure has been amended from the prior year. The previous wording was "Notified privacy breaches that are likely to cause serious harm, are followed up with the notifying agency within 10 working days of receipt". No change is required to be made on the prior year's results due to the amended wording. The previous target for this measure was 100% and it was reported as "Not achieved" in the Annual Report for the year ended 30 June 2024.

12. The target for this measure has been amended from the prior year. The previous target was 90%.

13. The sample of files selected were reviewed in line with the Compliance and Regulatory Action Framework and Compliance Notice Guidelines and an assessment was made against the quality standards. Each file was assigned a score from 1 to 5 with 1 being unacceptable and 5 being outstanding. An overall average score was calculated across all files reviewed and this was based on the judgement of the reviewer.

14. The wording for this measure has been amended from the prior year. The previous wording was "Incoming compliance issues are risk assessed to determine the appropriate response activity". No change is required to be made on the prior year result due to the amended wording. The previous target for this measure was 100% and it was reported as "Substantially achieved" in Annual Report for the year ended 30 June 2024.

## Function 4: Policy and Advocacy

### Activity areas of focus

Developing interventions such as guidance and Codes of Practice so that our expectations as a regulator are clear. We provide advice on the primary implications of policies being developed by government. We advocate for privacy positive outcomes.

### Output Measures

Measure	Estimate	Achieved 2024/25	Achieved 2023/24
The percentage of externally reviewed policy files that are rated as 3.5 out of 5 or better for quality.	85%	<b>Achieved – 93%</b> The review was undertaken by an external consulting firm and the result is based on a review of a sample of 15 files selected by the reviewer. Criteria are set out below. <sup>15</sup>	<b>Achieved – 100%</b>
Undertake 2 projects relevant to setting privacy standards, expectations or guidance in the privacy system.	Achieved	<b>Achieved</b> Completed the Inquiry into Foodstuffs North Island trial use of Facial Recognition Technology. Completed the development of the Biometrics Processing Privacy Code (issued in August 2025). Developed guidance to help implement the new indirect notification principle that will be introduced by the Privacy Amendment Bill.	<b>Achieved</b> The Biometrics project has achieved a number of key milestones in the year and work will continue in 2024/25.  The Artificial Intelligence project was completed during the year.
All externally reviewed policy files appropriately incorporate Treaty and Te Ao Māori analysis as necessary. <sup>16</sup>	85%	<b>Achieved</b> The reviewer noted that while there was limited consideration of te Ao Māori perspectives and Treaty of Waitangi, where te Ao Māori perspectives were covered, the work was well done.	<b>Achieved</b>

15. The files were reviewed against the quality standards established by the Policy Project and required for all government agencies with policy appropriations from July 2019. The assessment focussed on context, analysis, advice and actions outlined in each file reviewed. It also included an assessment of the incorporation of Treaty and Te Ao Māori analysis as necessary. Each file was assigned a score from 1 to 5 with 1 being unacceptable and 5 being outstanding. An overall average score was calculated across all files reviewed and this was based on the judgement of the reviewer.

16. The target for this measure has been amended from the previous year. The previous target was 100%.

## Function 5: Investigations and Dispute Resolution

### Activity areas of focus

Working with parties to achieve a fair outcome using dispute resolution techniques in the first instance. Investigating individual complaints where dispute resolution is inappropriate or unsuccessful. Declining to investigate cases where investigations are unnecessary or inappropriate. Referring serious cases to the Director of Human Rights Proceedings to consider bringing to the Human Rights Review Tribunal.

### Output Measures

Measure	Estimate	Achieved 2024/25	Achieved 2023/24
The percentage of notified complaint files closed by settlement between the parties.	50%	<b>Achieved – 67%</b>	<b>Achieved – 78%</b> The office has continued to focus on reaching settlement in the year.
The percentage of externally reviewed complaint investigations that are rated as 3.5 out of 5 or better for quality. <sup>17</sup>	85%	<b>Substantially achieved – 80%</b> The review was undertaken by a Barrister external to the Office and the result is based on a review of a sample of 20 files closed in the year selected by the reviewer. The average score for the files reviewed was “3.6 out of 5”. 100% of the files were rated 3.1 or higher, 80% of the files were rated 3.5 or higher. <sup>18</sup>	<b>Not achieved – 67%</b>
The percentage of complaints closed during the year that were less than 6 months old at closure. <sup>19</sup>	85%	<b>Achieved – 88%</b> There were 1,221 “Fast Resolve” complaints included in the calculation of this measure, of this 1,215 were resolved in less than 6 months.	<b>Not achieved – 75%</b> There were 1,028 “Fast Resolve” complaints included in the calculation of this measure. Of these 1,010 were resolved in less than 6 months.

17. The target for this measure has been amended from the previous year. The previous target was 90%.

18. Files were assessed for quality of legal analysis, correctness of legal conclusions, processes according to the law, processes according to best investigative/resolution/determinative practice and staff are following OPC policies in handling complaints. Each area was assigned a score of between 1 to 5 with 1 being not acceptable and 5 being outstanding. The scoring was based on the judgement of the reviewer. An average for each file was then calculated.

19. During this year, some discrepancies were identified in the way data for ‘fast resolve’ complaints were being captured. These have been rectified, and appropriate system amendments made. The changes have improved the prior year’s result from 69% to 75%.

# Statement of accounting policies

for the year ended 30 June 2025

## Reporting entity

These are the financial statements of the Privacy Commissioner, a Crown entity in terms of the Public Finance Act 1989 and the Crown Entities Act 2004. As such the Privacy Commissioner's ultimate parent is the New Zealand Crown.

These financial statements have been prepared in accordance with the requirements of the Crown Entities Act 2004.

The Privacy Commissioner's primary objective is to provide public services to the New Zealand public, as opposed to that of making a financial return. Accordingly, the Privacy Commissioner has designated itself as a public benefit entity for financial reporting purposes.

The financial statements for the Privacy Commissioner are for the year ended 30 June 2025 and were approved by the Commissioner on 24 October 2025. The financial statements cannot be altered after they have been authorised for issue.

## Basis of preparation

The financial statements have been prepared on a going concern basis, and the accounting policies have been applied consistently throughout the period.

## Statement of compliance

The financial statements of the Privacy Commissioner have been prepared in accordance with the requirements of the Crown Entities Act 2004, which includes the requirement to comply with New Zealand generally accepted accounting practice ("NZ GAAP").

The financial statements have been prepared in accordance with Tier 2 PBE accounting standards. The Tier 2 criteria have been met as expenditure is less than \$33m and the Privacy Commissioner is not publicly accountable (as defined in XRB A1 Accounting Standards Framework).

These financial statements comply with PBE accounting standards.

## Measurement base

The financial statements have been prepared on a historical cost basis.

## Functional and presentation currency

The financial statements are presented in New Zealand dollars and all values are rounded to the nearest thousand dollars (\$000). The functional currency of the Privacy Commissioner is New Zealand dollars.

## Summary of significant accounting policies

Significant accounting policies are included in the notes to which they relate. Significant accounting policies that do not relate to specific notes are outlined below.

### Budget figures

The budget figures are derived from the Statement of Performance Expectations as approved by the Privacy Commissioner at the beginning of the financial year.

The budget figures have been prepared in accordance with generally accepted accounting practice and are consistent with the accounting policies adopted by the Privacy Commissioner for the preparation of the financial statements.

### Cost allocation

The Privacy Commissioner has determined the costs of outputs using a cost allocation system as outlined below.

Direct costs are those costs directly attributed to an output. These costs are therefore charged directly to the outputs.

Indirect costs are those costs that cannot be identified in an economically feasible manner with a specific output. Personnel costs are charged based on % of time spent in relation to each output area. Other indirect costs are allocated based on the proportion of staff costs for each output area.

There have been no substantial changes to the cost allocation methodology since the date of the last audited financial statements.

### **Goods and Services Tax (GST)**

All items in the financial statements presented are exclusive of GST, with the exception of accounts receivable and accounts payable, which are presented on a GST inclusive basis. Where GST is irrecoverable as an input tax, then it is recognised as part of the related asset or expense.

The net amount of GST recoverable from, or payable to, the Inland Revenue Department (IRD) is included as part of receivables or payables in the statement of financial position.

The net GST paid to, or received from IRD – including the GST relating to investing and financing activities – is classified as an operating cash flow in the statement of cash flows.

Commitments and contingencies are disclosed exclusive of GST.

### **Income tax**

The Privacy Commissioner is a public authority for tax purposes and therefore exempt from income tax. Accordingly, no provision has been made for income tax.

### **Financial instruments**

The Privacy Commissioner is party to financial instruments as part of its normal operations. These financial instruments include bank accounts, short-term deposits, debtors, and creditors. All financial instruments are recognised in the statement of financial position and all revenues and expenses in relation to financial instruments are recognised in the statement of comprehensive revenue and expenses.

### **Critical accounting estimates and assumptions**

In preparing these financial statements the Privacy Commissioner has made estimates and assumptions concerning the future. These estimates and assumptions may differ from the subsequent actual results. Estimates and assumptions are continually evaluated and are based on historical experience and other factors, including expectations of future events that are believed to be reasonable under the circumstances.

The estimates and assumptions that have a significant risk of causing a material adjustment to the carrying amounts of assets and liabilities within the next financial year are:

- useful lives and residual values of property, plant and equipment – refer to Note 8
- useful lives of Software assets – refer to Note 9.

### **Critical judgements in applying the Privacy Commissioner's accounting policies**

Management has exercised the following critical judgements in applying the Privacy Commissioner's accounting policies for the period ended 30 June 2025:

- Lease classification – Refer Note 4
- Non-Government grants – Refer Note 2
- Grant expenditure – Refer Note 4

# Statement of comprehensive revenue and expenses

for the year ended 30 June 2025

	Note	Actual 2025 \$000	Budget 2025 \$000	Actual 2024 \$000
<b>Revenue</b>				
Crown revenue		7,640	7,640	8,171
Other revenue	2	195	146	266
<b>Total income</b>		<b>7,835</b>	<b>7,786</b>	<b>8,437</b>
<b>Expenditure</b>				
Promotion	4	116	119	62
Audit fees		57	53	53
Depreciation and amortisation	4,8,9	99	85	194
Rental expense		557	551	502
Operating expenses	4	1,029	1,294	1,275
Contract services		309	87	357
Staff expenses	3	5,920	6,300	6,150
<b>Total expenditure</b>		<b>8,087</b>	<b>8,489</b>	<b>8,593</b>
<b>Surplus/(Deficit)</b>		<b>(252)</b>	<b>(703)</b>	<b>(156)</b>
Other comprehensive revenue and expenses		-	-	-
<b>Total comprehensive revenue and expenses</b>		<b>(252)</b>	<b>(703)</b>	<b>(156)</b>

# Statement of changes in equity

for the year ended 30 June 2025

	Note	Actual 2025 \$000	Budget 2025 \$000	Actual 2024 \$000
Public Equity as at 1 July		2,441	2,417	2,597
Total comprehensive income		(252)	(703)	(156)
<b>Public equity as at 30 June</b>	<b>5</b>	<b>2,189</b>	<b>1,714</b>	<b>2,441</b>

Explanations of major variances are provided in Note 1

The accompanying notes and accounting policies form part of these financial statements



# Statement of financial position

as at 30 June 2025

	Note	Actual 2025 \$000	Budget 2025 \$000	Actual 2024 \$000
<b>Public Equity</b>				
General funds	5	2,189	1,714	2,441
<b>Total public equity</b>		<b>2,189</b>	<b>1,714</b>	<b>2,441</b>
<b>Current assets</b>				
Cash and cash equivalents	6	2,271	1,808	2,574
Receivables	7	64	33	62
Prepayments	7	127	114	126
<b>Total current assets</b>		<b>2,462</b>	<b>1,955</b>	<b>2,762</b>
<b>Non-current assets</b>				
Property, plant and equipment	8	134	173	223
Intangible assets	9	4	24	2
<b>Total non-current assets</b>		<b>138</b>	<b>197</b>	<b>225</b>
<b>Total assets</b>		<b>2,600</b>	<b>2,152</b>	<b>2,987</b>
<b>Current liabilities</b>				
Payables	10	194	164	274
Employee entitlements	12	217	270	270
<b>Total current liabilities</b>		<b>411</b>	<b>434</b>	<b>544</b>
<b>Non-current liabilities</b>				
Lease incentive – non current	11	-	4	2
<b>Total non-current liabilities</b>		<b>-</b>	<b>4</b>	<b>2</b>
<b>Total liabilities</b>		<b>411</b>	<b>438</b>	<b>546</b>
<b>Net assets</b>		<b>2,189</b>	<b>1,714</b>	<b>2,441</b>

Explanations of major variances are provided in Note 1

The accompanying notes and accounting policies form part of these financial statements

# Statement of cash flows

for the year ended 30 June 2025

	Note	Actual 2025 \$000	Budget 2025 \$000	Actual 2024 \$000
<b>CASH FLOWS FROM OPERATING ACTIVITIES</b>				
<b>Cash was provided from:</b>				
Receipts from the Crown		7,640	7,640	8,171
Receipts from other revenue		116	116	174
Interest received		79	30	117
		<b>7,835</b>	<b>7,786</b>	<b>8,462</b>
<b>Cash was applied to:</b>				
Payment to suppliers		2,156	2,065	2,122
Payments to employees		5,973	6,282	6,127
Net Goods and Services Tax		(3)	(30)	4
		<b>8,126</b>	<b>8,317</b>	<b>8,253</b>
<b>Net cash flows from operating activities</b>		<b>(291)</b>	<b>(531)</b>	<b>209</b>
<b>CASH FLOWS FROM INVESTING ACTIVITIES</b>				
<b>Cash was applied to:</b>				
Purchase of property, plant and equipment and intangibles		12	50	24
<b>Cash was provided from:</b>				
Sale of property, plant and equipment and intangibles		-	-	-
<b>Net cash flows from investing activities</b>		<b>(12)</b>	<b>(50)</b>	<b>(24)</b>
Net increase/(decrease) in cash held		(303)	(581)	185
Plus opening cash		2,574	2,389	2,389
<b>Closing cash balance</b>	6	<b>2,271</b>	<b>1,808</b>	<b>2,574</b>
<b>Cash and bank</b>		<b>2,271</b>	<b>1,808</b>	<b>2,574</b>

The GST (net) component of operating activities reflects the net GST paid and received with the Inland Revenue Department. The GST (net) component has been presented on a net basis, as the gross amounts do not provide meaningful information for financial statement purposes.

The accompanying notes and accounting policies form part of these financial statements

# Notes to the financial statements

for the year ended 30 June 2025

## Note 1: Explanation of major variances against budget

Explanations for significant variations from the Privacy Commissioner's budgeted figures in the Statement of Performance Expectations are as follows:

### Statement of comprehensive revenue and expenses

The year-end reported a deficit lower than the budgeted by \$451k. This is primarily due to the following:

#### Interest (up on budget by \$49k)

Interest income has exceeded budget as a result of cash reserves in the bank and higher interest rates.

#### Staff expenses (down on budget by \$380k)

Staff departures and a number of vacancies have resulted in the salary costs being lower than budgeted.

#### Contract services (up on budget by \$222k)

The main increase against budget is due to the Office engaging contractors to assist in advancing work in our capability and guidance and legal area where some positions were vacant.

#### Other operating expenses (down on budget by \$265k)

The under budget variance was mainly due to lower computer and network expenses as the result of some one-off costs not eventuating and saving from other areas.

## Note 2: Revenue

### Accounting policy

The specific accounting policies for significant revenue items are explained below:

#### Revenue from the Crown

The Privacy Commissioner is primarily funded through revenue received from the Crown, which is restricted in its use for the purpose of the Privacy Commissioner meeting his/her objectives as specified in the Statement of Intent and Statement of Performance Expectations.

The Privacy Commissioner considers there are no conditions attached to the funding and it is recognised as revenue at the point of entitlement.

The fair value of revenue from the Crown has been determined to be equivalent to the amounts due in the funding arrangements.

#### Other grants

Non-government grants are recognised as revenue when they become receivable unless there is an obligation in substance to return the funds if conditions of the grant are not met. If there is such an obligation the grants are initially recorded as grants received in advance and recognised as revenue when conditions of the grant are satisfied.

#### Interest

Interest revenue is recognised by accruing on a time proportion basis.

#### Provision of services

Revenue derived through the provision of services to third parties is treated as exchange revenue and recognised in proportion to the stage of completion at the balance sheet date.

## Critical judgements in applying accounting policies

### Non-government grants

The Privacy Commissioner must exercise judgement when recognising grant income to determine if conditions of the grant contract have been satisfied. This judgement will be based on the facts and circumstances that are evident for each grant contract.

### Crown revenue

The Privacy Commissioner has been provided with funding from the Crown for specific purposes of the Privacy Commissioner as set out in its founding legislation and the scope of the relevant government appropriations. Apart from these general restrictions, there are no unfulfilled conditions or contingencies attached to government funding (2024: \$nil).

### Other revenue breakdown

	Actual 2025 \$000	Actual 2024 \$000
Other grants received	116	116
Other revenue	-	33
Interest revenue	79	117
<b>Total other revenue</b>	<b>195</b>	<b>266</b>

## Note 3: Staff expenses

### Accounting policy

#### Superannuation schemes

##### *Defined contribution schemes*

Obligations for contributors to Kiwi Saver and the Government Superannuation Fund are accounted for as defined contribution superannuation schemes and are recognised as an expense in the statement of comprehensive revenue and expenses as incurred.

### Breakdown of staff costs and further information

	Actual 2025 \$000	Actual 2024 \$000
Salaries and wages	5,736	5,894
Employer contributions to defined contribution plans	193	189
Other staff expenses	44	44
Increase/(decrease) in employee entitlements	(53)	23
<b>Total staff expenses</b>	<b>5,920</b>	<b>6,150</b>

## Note 4: Other expenses

### Accounting policy

#### Operating leases

Operating lease expenses are recognised on a straight-line basis over the term of the lease.

### Critical judgements in applying accounting policies

#### Lease classification

Determining whether a lease is to be treated as an operating lease or a finance lease requires some judgement. Leases where the lessor effectively retains substantially all the risks and benefits of ownership of the leased items are classified as operating leases.

### Other expenses and further information

The total comprehensive revenue and expenses is after charging for the following significant expenses:

	Actual 2025 \$000	Actual 2024 \$000
<b>Fees paid to auditors:</b>		
External audit	57	53
<b>Promotions costs:</b>		
Website expenses	100	28
Privacy Week/Forum	3	4
Other marketing expenses	13	30
<b>Total promotion expenses</b>	<b>116</b>	<b>62</b>
<b>Depreciation and amortisation:</b>		
Furniture and fittings	57	55
Computer and equipment	32	39
Office equipment	6	11
Intangibles	4	89
<b>Total depreciation and amortisation</b>	<b>99</b>	<b>194</b>
Rental expense on operating leases	557	502
Contract services	309	357
<b>Other operating expenses:</b>		
Computer maintenance/licences	277	332
Staff travel	67	67
Staff development	57	64
Loss on disposal	-	1
Recruitment	22	29
Utilities	328	419
Other	278	363
<b>Total other operating expenses</b>	<b>1,029</b>	<b>1,275</b>

## Operating leases as lessee

The future aggregate minimum lease payments to be paid under non-cancellable leases are as follows:

	Actual 2025 \$000	Actual 2024 \$000
Not later than one year	537	564
Later than one year and not later than five years	595	655
Later than five years	-	-
<b>Total non-cancellable operating leases</b>	<b>1,132</b>	<b>1,219</b>

The Privacy Commissioner leases two properties, one in Wellington and the other in Auckland. The Wellington lease will expire in December 2026 and the Auckland lease has been renewed and will expire in December 2028.

A lease incentive was offered as part of the current Auckland lease. This is being accounted for in line with PBE IPSAS 13 Leases.

During 2022, the Privacy Commissioner negotiated a new agreement for the lease of Zoom Room equipment. The term was for 24 months and this was further extended to October 2025.

In April 2024, the Privacy Commissioner has entered into a lease agreement for the lease of its printers. The term is 60 months ending April 2029.

The Privacy Commissioner does not have the option to purchase the assets at the end of the lease term.

There are no restrictions placed on the Privacy Commissioner by any of its leasing arrangements.

## Note 5: General funds

	Actual 2025 \$000	Actual 2024 \$000
Opening balance	2,441	2,597
Net (deficit)/surplus	(252)	(156)
<b>Closing balance</b>	<b>2,189</b>	<b>2,441</b>

## Note 6: Cash and cash equivalents

### Accounting policy

Cash and cash equivalents include cash on hand, deposits held at call with banks both domestic and international, other short-term, highly liquid investments, with original maturities of three months or less and bank overdrafts.

	Actual 2025 \$000	Actual 2024 \$000
Cash on hand and at bank	110	98
Cash equivalents – on call accounts	2,161	2,476
<b>Total cash and cash equivalents</b>	<b>2,271</b>	<b>2,574</b>

The carrying value of short-term deposits with maturity dates of three months or less approximates their fair value.

## Note 7: Receivables

### Accounting policy

Short-term debtors and receivables are recorded at their fair value, less an allowance for expected losses.

	Actual 2025 \$000	Actual 2024 \$000
Receivables	64	62
Prepayments	127	126
<b>Total</b>	<b>191</b>	<b>188</b>
<b>Total receivables comprises</b>		
GST receivable (exchange transaction)	64	62
Other receivables (exchange transaction)	-	-
<b>Total</b>	<b>64</b>	<b>62</b>

The carrying value of receivables approximates their fair value.

## Note 8: Property, plant and equipment and further information

### Accounting policy

Property, plant and equipment asset classes consist of furniture and fittings, computer equipment, and office equipment.

Property, plant and equipment are shown at cost less any accumulated depreciation and impairment losses.

### Depreciation

Depreciation is provided on a straight-line basis on all property, plant and equipment, at a rate which will write off the cost of the assets to their estimated residual value over their useful lives.

The useful lives and associated depreciation rates of major classes of assets have been estimated as follows:

Furniture and fittings	5 – 7 years
Computer equipment	4 years
Office equipment	5 years

### Additions

The cost of an item of property, plant and equipment is recognised as an asset only when it is probable that future economic benefits or service potential associated with the item will flow to the Privacy Commissioner and the cost of the item can be measured reliably.

Where an asset is acquired through a non-exchange transaction (at no cost), or for a nominal cost, it is recognised at fair value when control over the asset is obtained.

Costs incurred after initial acquisition are capitalised only when it is probable that future economic benefits or service potential associated with the item will flow to the Privacy Commissioner and the cost of the item can be measured reliably.

The costs of day-to-day servicing of property, plant and equipment are recognised in the statement of comprehensive revenue and expenses as they are incurred.

### Disposals

Gains and losses on disposals are determined by comparing the proceeds with the carrying amount of the asset. Gains and losses on disposals are included in the statement of comprehensive revenue and expenses.

### Impairment of property, plant and equipment

Property, plant and equipment and intangible assets that have a finite useful life are reviewed for impairment whenever events or changes in circumstances indicate that the carrying amount may not be recoverable. An impairment loss is recognised for the amount by which the asset's carrying amount exceeds its recoverable amount. The recoverable amount is the higher of an asset's fair value less costs to sell and value in use.

Value in use is the depreciated replacement cost for an asset where the future economic benefits or service potential of the asset are not primarily dependent on the asset's ability to generate net cash inflows and where the Privacy Commissioner would, if deprived of the asset, replace its remaining future economic benefits or service potential.

If an asset's carrying amount exceeds its recoverable amount, the asset is impaired and the carrying amount is written down to the recoverable amount.

For assets not carried at a revalued amount, the total impairment loss is recognised in the statement of comprehensive revenue and expenses.

### Critical accounting estimates and assumptions

#### Estimating useful lives and residual values of property, plant and equipment

At each balance date the Privacy Commissioner reviews the useful lives and residual values of its property, plant and equipment. Assessing the appropriateness of useful life and residual value estimates of property, plant and equipment requires the Privacy Commissioner to consider a number of factors such as the physical condition of the asset, expected period of use of the asset by the Privacy Commissioner, and expected disposal proceeds from the future sale of the asset.

An incorrect estimate of the useful life or residual value will impact the depreciation expense recognised in the statement of comprehensive revenue and expenses and carrying amount of the asset in the statement of financial position.



The Privacy Commissioner minimises the risk of this estimation uncertainty by:

- physical inspection of assets
- asset replacement programmes
- review of second-hand market prices for similar assets; and
- analysis of prior asset sales.

The Privacy Commissioner has not made significant changes to past assumptions concerning useful lives and residual values.

	Furniture and fittings \$000	Computer equipment \$000	Office equipment \$000	Total \$000
<b>Cost</b>				
Balance at 1 July 2023	306	189	88	583
Additions	18	6	-	24
Disposals	-	-	(27)	(27)
<b>Balance at 30 June 2024</b>	<b>324</b>	<b>195</b>	<b>61</b>	<b>580</b>
Additions	-	6	-	6
Disposals	-	(14)	(5)	(19)
<b>Balance at 30 June 2025</b>	<b>324</b>	<b>187</b>	<b>56</b>	<b>567</b>
<b>Accumulated depreciation</b>				
Balance at 1 July 2023	113	104	61	278
Depreciation expense	55	39	11	105
Elimination on disposal	-	-	(26)	(26)
<b>Balance at 30 June 2024</b>	<b>168</b>	<b>143</b>	<b>46</b>	<b>357</b>
Depreciation expense	57	32	6	95
Elimination on disposal	-	(14)	(5)	(19)
<b>Balance at 30 June 2025</b>	<b>225</b>	<b>161</b>	<b>47</b>	<b>433</b>
<b>Carrying amounts</b>				
<b>At 1 July 2024</b>	<b>156</b>	<b>52</b>	<b>15</b>	<b>223</b>
<b>At 30 June 2025</b>	<b>99</b>	<b>26</b>	<b>9</b>	<b>134</b>

There are no restrictions over the title of the Privacy Commissioner's property, plant and equipment, nor are any pledged as security for liabilities.

### Capital commitments

The Privacy Commissioner has capital commitments of \$nil as at 30 June 2025. (2024: \$nil).

## Note 9: Intangible assets

### Accounting policy

#### Software acquisition

Acquired computer software licenses are capitalised based on the costs incurred to acquire and bring to use the specific software and only when the license covers a period of over 2 years.

Costs associated with maintaining computer software are recognised as an expense when incurred.

#### Website costs

Costs that are directly associated with the development of interactive aspects of the Office's website are capitalised when they are ready for use.

Costs associated with general maintenance and development of non-interactive aspects of the Office's website are recognised as an expense as incurred.

#### Amortisation

The carrying value of an intangible asset with a finite life is amortised on a straight-line basis over its useful life. Amortisation begins when the asset is available for use and ceases at the date that the asset is derecognised. The amortisation charge for each period is recognised in the statement of comprehensive revenue and expenses.

The useful lives and associated amortisation rates of major classes of intangible assets have been estimated as follows:

Acquired computer software	2–4 years
Interactive tools	3 Years

The software is amortised over the length of the licence.

#### Impairment

Refer to the policy for impairment of property, plant and equipment in Note 8. The same approach applies to the impairment of intangible assets.

### Critical accounting estimates and assumptions

#### Estimating useful lives of software assets

The Office's capitalised interactive website tools comprise of a number of interactive website tools and e-learning modules that have been capitalised over the past 6 years. The tools were mainly developed by external providers. These tools have a finite life, which requires the Office to estimate the useful life of the assets.

In assessing the useful lives of these tools, several factors are considered, including: the effect of technological change on systems and platforms, and the expected timeframe for the development of replacement systems and platforms.

An incorrect estimate of the useful lives of these assets will affect the amortisation expense recognised in the surplus or deficit, and the carrying amount of the assets in the statement of financial position.

Taking the above into account the Office has estimated a useful life of three years for these interactive tools and there are currently no indicators that the period of use of the tools will be materially different.

#### Treatment of software-as-a-service arrangements

The IASB's Interpretation Committee issued an agenda decision in April 2021 that clarified the accounting treatment expected under the International Financial Reporting Standards for customisation and configuration costs associated with software as a service (SaaS) arrangements.

Where software is provided under a Software-as-a-service (SaaS) arrangement, costs of configuration and customisation are recognised as an intangible asset only if the activities create an intangible asset that the Privacy Commissioner controls and asset recognition criteria are met. Costs, including ongoing fees for use of software, that do not result in an intangible asset or a software finance lease are expensed as a service contract as incurred. However, where fees represent payment for future services to be received, the Privacy Commissioner recognises these as a prepayment and expenses these as subsequent services are received.

Staff training costs are recognised as an expense when incurred.

There have been 6k of Interactive tools capitalisation in the year to 30 June 2025 (2024: \$nil).

	Acquired software \$000	Interactive Tools \$000	Total \$000
<b>Cost</b>			
Balance at 1 July 2023	92	652	744
Additions	-	-	-
Disposals	-	-	-
<b>Balance at 30 June 2024</b>	<b>92</b>	<b>652</b>	<b>744</b>
Additions	-	6	6
Disposals	(19)	-	(19)
<b>Balance at 30 June 2025</b>	<b>73</b>	<b>658</b>	<b>731</b>
<b>Accumulated depreciation</b>			
Balance at 1 July 2023	87	566	653
Depreciation expense	5	84	89
Elimination on disposal	-	-	-
<b>Balance at 30 June 2024</b>	<b>92</b>	<b>650</b>	<b>742</b>
Depreciation expense	-	4	4
Elimination on disposal	(19)	-	(19)
<b>Balance at 30 June 2025</b>	<b>73</b>	<b>654</b>	<b>727</b>
<b>Carrying amounts</b>			
<b>At 1 July 2024</b>	<b>-</b>	<b>2</b>	<b>2</b>
<b>At 30 June 2025</b>	<b>-</b>	<b>4</b>	<b>4</b>

There are no restrictions over the title of the Privacy Commissioner's intangible assets, nor are any intangible assets pledged as security for liabilities.

## Capital Commitments

The Privacy Commissioner has capital commitments of \$nil as at 30 June 2025. (2024: \$nil).

## Note 10: Payables

### Accounting policy

Creditors and other payables are recorded at the amount payable.

	Actual 2025 \$000	Actual 2024 \$000
<b>Payables under exchange transactions</b>		
Creditors	100	117
Accrued expenses	91	150
Lease incentive	3	7
<b>Total Payables under exchange transactions</b>	<b>194</b>	<b>274</b>
<b>Total creditors and other payables</b>	<b>194</b>	<b>274</b>

There were no payables under non-exchange transactions (2024 \$nil).

Creditors and other payables are non-interest bearing and are normally settled on **30-day terms**, therefore the carrying value of creditors and other payables approximates their fair value.

## Note 11: Non-current liabilities

	Actual 2025 \$000	Actual 2024 \$000
Lease incentive	-	2
<b>Total non-current liabilities</b>	<b>-</b>	<b>2</b>

Lease incentive for the Auckland office for the period 1 December 2019 to 30 November 2025 (6-year lease).

## Note 12: Employee entitlements

### Accounting policy

Employee entitlements that the Privacy Commissioner expects to be settled wholly within 12 months after the end of the reporting period in which the employees render the related service, are measured based on accrued entitlements at current rates of pay.

These include salaries and wages accrued up to balance date and annual leave earned but not yet taken at balance date, expected to be settled within 12 months.

	Actual 2025 \$000	Actual 2024 \$000
<b>Current employee entitlements are represented by:</b>		
Accrued salaries and wages	22	16
Annual leave	195	254
<b>Total employee entitlement</b>	<b>217</b>	<b>270</b>
Current	217	270
Non-current		
<b>Total employee entitlements</b>	<b>217</b>	<b>270</b>

## Note 13: Contingencies

There are no known contingencies existing at balance date (2024: \$nil).

## Note 14: Related party information

The Privacy Commissioner is a wholly owned entity of the Crown. The Government significantly influences the role of the Privacy Commissioner as well as being its major source of revenue.

Related party disclosures have not been made for transactions with related parties that are within a normal supplier or client/recipient relationship on terms and conditions no more or less favourable than those that it is reasonable to expect the Privacy Commissioner would have adopted in dealing with the party at arm's length in the same circumstances. Further, transactions with other government agencies (for example, government departments and Crown entities) are not disclosed as related party transactions when they are consistent with the normal operating arrangements between government agencies and undertaken on the normal terms and conditions for such transactions.

There were no other related party transactions.

	Actual 2025 \$000	Actual 2024 \$000
<b>Key management personnel compensation</b>		
Total Salaries and other short-term employee benefits	1,201	1,362
Full-time equivalent members	4.0	4.9

## Note 15: Post balance date events

There are no other adjusting events after balance date of such importance that non-disclosure would affect the ability of the users of the financial report to make proper evaluations and decisions.

## Note 16: Financial instruments

### 16A Financial instrument categories

The carrying amounts of financial assets and liabilities in each of the financial instrument categories are as follows:

	Actual 2025 \$000	Actual 2024 \$000
<b>FINANCIAL ASSETS</b>		
<b>Financial assets measured at amortised cost</b>		
Cash and cash equivalents	2,271	2,574
Receivables (excluding prepayments and taxes receivables)	-	-
<b>Total financial assets</b>	<b>2,271</b>	<b>2,574</b>
<b>FINANCIAL LIABILITIES</b>		
<b>Financial liabilities measured at amortised costs</b>		
Payables (excluding income in advance, taxes payable. Grants	191	267
<b>Total financial liabilities</b>	<b>191</b>	<b>267</b>

# Appendices | Ngā Tāpiritanga

## Appendix A | Tāpiritanga A

### Statutory review of information matching provisions

The Privacy Act requires that the Commissioner review the operation of each information matching provision every five years. In these reviews under s.184 the Commissioner recommends whether a provision should continue, be amended or be cancelled.

During the reporting period, I reviewed the seven information matching provisions that the Ministry of Social Development (MSD) uses to verify eligibility, to trace debtors, and to assist the Ministry of Justice in getting people with outstanding warrants to engage with the justice system. The provisions reviewed and the respective outcomes are:

#### Accident Compensation Act 2001, s 281

This provision permits MSD to identify individuals whose entitlement may have changed because they are receiving Accident Compensation Corporation (ACC) payments, and to assist MSD in the recovery of outstanding debts.

I consider that the authority conferred by section 281 of the Accident Compensation Act 2001 should be continued without amendment.

### Births, Deaths, Marriages, and Relationships Registration Act 1995, s 78A and Schedule 1A

This provision permits the Department of Internal Affairs to disclose birth, marriage, civil union, name change and death information to MSD to verify a person's eligibility or continuing eligibility, and to identify debtors.

I consider that the authority conferred by section 78A and Schedule 1A of the Births, Deaths, Marriages, and Relationships Registration Act should be continued without amendment.

#### Corrections Act 2004, s 180

This provision permits MSD to detect people who are receiving income support payments while imprisoned, and to assist MSD in the recovery of outstanding debts.

I consider that the authority conferred by section 180 of the Corrections Act 2004 should be continued without amendment.

### **Customs and Excise Act 2018, s 308**

This provision permits MSD to identify current clients who leave for or return from overseas while receiving income support payments, and to assist MSD in the recovery of outstanding debts. When section 308 was re-drafted from the previous section 280 of the prior 1996 Act, the information flow was changed in the drafting despite there not being any change in the matching activity.

This provision was superseded by an information sharing agreement in May 2019 and should be repealed.

### **Education Act 1989, s 226A and s 235F**

This provision allows MSD StudyLink to verify student enrolment information, from public and private educational institutions respectively, to confirm entitlement to allowances and loans.

I consider that the authority conferred by sections 226A and 235F of the Education Act 1989 should be continued without amendment.

### **Education Act 1989, s 307D**

This provision permits MSD to determine eligibility for student loans and/or allowance by verifying students' study results.

I consider that the authority conferred by section 307D Education Act 1989 should be continued without amendment.

### **Social Security Act 2018 schedule 6, cl 15**

This provision enables MSD to suspend or reduce the benefits of people who have an outstanding warrant to arrest for criminal proceedings as an incentive for the individual to resolve the warrant.

I consider that the authority conferred by the Social Security Act 2018 schedule 6 clause 15 should be continued without amendment.

## **Assurance overview of the information matching programmes**

Information matching provisions are authorised by statute and listed in Schedule 5 of the Privacy Act 2020. The Privacy Commissioner has a regulatory role to monitor the use of information matching by government departments. We do this by completing an annual assurance review of the operation of the matching programmes. The Commissioner must also review each information matching provisions every five years to identify any amendments required and if the provision itself should be continued.

Our assessment of a matching programme's compliance is based on the information provided to us by agencies as part of regular reporting, and any other issues drawn to our attention during the reporting period. From time to time, we will actively seek more detailed evidence of compliance with particular rules.

## **Current programmes**

There were 42 information matching programmes in operation during the period, and 11 programmes that were not active.

### *Inactive programmes*

1. The Electoral Commission did not operate their programme of five matches to invite people to enrol under the Electoral Act 1993, s 263B.
  - DIA (Citizenship)/EC Unenrolled Voters
  - DIA (Passports)/EC Unenrolled Voters
  - MSD/EC Unenrolled Voters
  - NZTA (Driver Licence)/EC Unenrolled Voters
  - NZTA (Vehicle Registration)/EC Unenrolled Voters
2. The Ministry of Health did not operate the Publicly Funded Health Eligibility match under the Immigration Act 2009, s 300. MOH had intended to this match in the 2024/2025 year, however this did not occur. MOH has not confirmed a schedule for the match in 2025-2026. OPC will review the ongoing requirement for the matching provision at the next five yearly review.



3. The Ministry of Justice did not operate the Fines Defaulters Tracing match with Immigration NZ under s 295 of the Immigration Act 2009. There are no plans to reinstate this match. On this basis, in August 2023, the Commissioner recommended that this programme is repealed, which requires a legislative change to the Immigration Act. MoJ no longer provides information to OPC on this match other than a statement advising that it is no longer active in its annual reporting.
4. The Ministry for Business, Innovation and Employment did not operate the match to identify unlicensed motor vehicle traders under Motor Vehicle Sales Act 2003, s 120 and s 121 with Customs Service. The match has not operated for the last 8 years and MBIE has no firm plans to discuss reactivating this information matching provision in the upcoming financial year. OPC will review the ongoing requirement for the matching provision at the next five yearly review.
5. The Ministry for Business, Innovation and Employment also did not operate the match under Motor Vehicle Sales Act 2003, s 122 and s 123 with the New Zealand Transport Agency. These matches were suspended while the programme was reviewed. An updated matching programme was restarted for the 2025–2026 period.
6. The Ministry for Social Development did not operate the Customs/MSD Periods of Residence Match with Australia under the Customs and Excise Act 2018, s 309, nor the Netherlands Tax Information Match under the Social Security Act 2018, s 380 and Social Welfare (Reciprocity with the Netherlands) Order 2003. The matching programme with Australia was suspended in 2012, and the matching programme with the Netherlands was suspended in 2011.

## New or ceased provisions and programmes:

Parliament passed no new information matching provisions during the year. No programmes were ceased.

## Assessment of active information matching programmes for 2024/2025

We describe programmes' compliance in the following manner:







**Compliant:** where the evidence we have been provided indicates that the programme complies with the information matching rules.



**Not compliant – minor technical issues:** where reporting has identified practices that are not compliant with the information matching rules, but genuine efforts have been made to implement a compliant programme, and the risks to individual privacy are low.



**Not compliant – substantive issues:** where reporting has identified practices that are not compliant with the information matching rules or other provisions of the Privacy Act that cannot be considered minor technical issues.

Information provided to Accident Compensation Corporation		Compliance rating
<b>1</b>	<p><b>IR / ACC Compensation and Levies</b></p> <p>To confirm income amounts for compensation calculations</p> <p><i>Accident Compensation Act 2001, s 246 and Tax Administration Act 1994, Schedule 7 Part C subpart 2 cl 41</i></p> <p>Inland Revenue (IR) disclosure to ACC: For self-employed people, IR provides ACC with the full name, contact details, date of birth, IR number and earnings information. For employers, IR provides ACC with the name, address, IR number, and total employee earnings.</p>	
<b>2</b>	<p><b>Corrections / ACC Prisoners</b></p> <p>To ensure that prisoners do not continue to receive earnings-related accident compensation payments</p> <p><i>Accident Compensation Act 2001, s 281</i></p> <p>Corrections disclosure to ACC: Corrections provides ACC with the surname, given names, date of birth, gender, date received in prison and any aliases of all people newly admitted to prison.</p>	
Information provided to Department of Internal Affairs		
<b>3</b>	<p><b>BDM/DIA(Citizenship) Citizenship Application Processing</b></p> <p>To verify a parent's citizenship status if required for determining an applicant's eligibility for New Zealand citizenship.</p> <p><i>Births, Deaths, Marriages, and Relationships Registration Act 2021 s 112</i></p> <p>BDM disclosure to Citizenship (DIA): Possible matches from the Births, Deaths, and Marriages (relationships) databases are displayed to Citizenship staff as they process each application. These details include full name, gender, date of birth, place of birth and parents' full names.</p>	
<b>4</b>	<p><b>DIA (Citizenship)/BDM Citizenship by Birth Processing</b></p> <p>To enable the Registrar-General to determine the citizenship-by-birth status of a person born in New Zealand on or after 1 January 2006, for the purpose of recording the person's citizenship status on his or her birth registration entry.</p> <p><i>Citizenship Act 1977, s 26A</i></p> <p>BDM disclosure to Citizenship (DIA): For birth registration applications, when no parental birth record can be found, a request is transferred electronically to the citizenship unit to be manually checked against the relevant citizenship records. The information supplied includes the child's date of birth, and parents' full names and birth details.</p> <p>Citizenship (DIA) disclosure to BDM: Citizenship responds to these requests by stating either the type of qualifying record found or that qualifying records were not found.</p>	

## 5 DIA Identity Verification Service (IVS)

To verify identity information provided by an applicant in support of their application for issuance, renewal, amendment, or cancellation of an Electronic Identity Credential, or to keep the core information contained in an EIC accurate and up to date.

*Electronic Identity Verification Act 2012, s 39*

Births disclosure to IVS: Child's names, gender, date of birth, place of birth, country of birth, citizenship by birth status, marriage date, registration number, mother's names, father's names, since died indicator and still born indicator.

Deaths disclosure to IVS: Names, gender, date of birth, place of birth, date of death, place of death and age at death.

Marriages disclosure to IVS: Names, date of birth, date of marriage, registration number, country of birth, gender, place of marriage, spouse's names.

Citizenship disclosure to IVS: Names, gender, date of birth, place of birth, photograph, citizenship person identifier, citizenship certificate number, certificate type and certificate status.

Passports disclosure to IVS: Names, gender, date of birth, place of birth, photograph, passport person identifier, passport number, date passport issued, date passport expired and passport status.

Immigration disclosure to IVS: Whether a match is found, client ID number and any of the pre-defined set of identity related alerts.



## Information provided to Electoral Commission

## 6 INZ/EC Unqualified Voters

To identify, from immigration records, those on the electoral roll who appear not to meet New Zealand residency requirements, so their names may be removed from the roll.

*Electoral Act 1993, s 263A*

INZ disclosure to the Electoral Commission (EC): INZ provides full name (including aliases), date of birth, address and permit expiry date. The type of permit can be identified because five separate files are received, each relating to a different permit type.



## Information provided to Immigration New Zealand

### 7 BDM (Deaths)/INZ Deceased Temporary Visa Holders

To identify and remove or update the records of people who are deceased from the Immigration New Zealand (INZ) database of overstayers and temporary permit holders.

*Births, Deaths, Marriages, and Relationships Registration Act 2021 s 112*

BDM provides information from the Deaths Register covering the six months prior to the extract date. The information includes full name at birth, full name at death, gender, birth date, death date, country of birth, and number of years lived in New Zealand.



### 8 DIA(Citizenship)/INZ Entitlement to Reside

To remove from the Immigration New Zealand (INZ) overstayer records the names of people who have been granted New Zealand citizenship.

Citizenship (DIA) disclosure to INZ: Citizenship provides information from the Citizenship Register about people who have been granted citizenship. Each record includes full name, gender, date of birth, country of birth and citizenship person number.



### 9 Corrections/INZ Prisoners

To identify prisoners who fall within the deportation provisions of the Immigration Act 2009 because of their criminal convictions or are subject to deportation because their visa to be in New Zealand has expired.

*Corrections Act 2004, s 181 and Immigration Act 2009, s 294*

Corrections disclosure to INZ: Corrections discloses information about all newly admitted prisoners. Each prisoner record includes full name (and known aliases), date and place of birth, gender, prisoner unique identifier, and name of the prison facility. Each prisoner's offence and sentence information is also included.

INZ disclosure to Corrections: For prisoners who are subject to removal or deportation orders, and who have no further means of challenging those orders, INZ discloses the full name, date and place of birth, gender, citizenship, prisoner unique identifier, immigration status and details of removal action that INZ intends to take.



## Information provided to Inland Revenue

### 10 BDM (Births)/IR Newborns Tax Number

To enable birth information to be confirmed to allocate an IR number to a new-born child.

*Births, Deaths, Marriages, and Relationships Registration Act 2021 s 112*

Births, Deaths and Marriages (BDM) disclosure to IR: The information includes the child's full name, sex, citizenship status and birth registration number. Additionally, the full name, address and date of birth of both mother and father are provided.



### 11 BDM (Deaths)/IR Deceased Taxpayers

To identify taxpayers who have died so that IR can close accounts where activity has ceased.

*Births, Deaths, Marriages, and Relationships Registration Act 2021 s 112*

BDM disclosure to IR: BDM provides death information including the full name, gender, date of birth, date of death, home address, death registration number and spouse's details.



### 12 Customs/IR Student Loan Alerts




To identify overseas based borrowers in serious default of their student loan repayment obligations who leave for, or return from, overseas so that IR can take steps to recover the outstanding debt.

*Customs and Excise Act 2018, s 306*

IR disclosure to Customs: IR provides Customs with the full name, date of birth, and IR number of borrowers in serious default of their student loan obligations.

Customs disclosure to IR: Customs provides IR with the person's arrival card information. This includes the full name, date of birth, and date, time and direction of travel including New Zealand port and prime overseas port (last port of call for arrivals and first port of call for departures).



<p><b>13</b></p>	<p><b>Customs/IR Student Loan Person of Interest</b></p> <p>To detect student loan borrowers who leave for, or return from, overseas so that IR can administer the student loan scheme and its interest-free conditions.</p> <p><i>Customs and Excise Act 2018, s 306</i></p> <p>IR disclosure to Customs: IR provides Customs with the full name, date of birth, and IR number for student loan borrowers who have a loan of more than \$20.</p> <p>Customs disclosure to IR: For possible matches to borrowers, Customs provides the full name, date of birth, IR number and date, time and direction of travel.</p>	
<p><b>14</b></p>	<p><b>Customs/IR Child Support Alerts</b></p> <p>To identify parents in serious default of their child support liabilities who leave for or return from overseas so that IR can take steps to recover the outstanding debt.</p> <p><i>Customs and Excise Act 2018, s 307</i></p> <p>IR disclosure to Customs: IR provides Customs with the full name, date of birth, and IR number of parents in serious default of their child support liabilities.</p> <p>Customs disclosure to IR: Customs provides IR with the person's arrival card information. This includes the full name, date of birth, and date, time and direction of travel including New Zealand port and prime overseas port (last port of call for arrivals and first port of call for departures).</p>	
<p><b>Information provided to Ministry of Education</b></p>		
<p><b>15</b></p>	<p><b>BDM (Births)/MoE Student Birth Confirmation</b></p> <p>To improve the quality and integrity of data held on the National Student Index (NSI) and reduce compliance costs for students by verifying their details for tertiary education organisations.</p> <p><i>Births, Deaths, Marriages, and Relationships Registration Act 2021 s 112</i></p> <p>BDM disclosure to Ministry of Education: BDM provides names, gender, date of birth of New Zealand- born citizens.</p> <p><i>Note:</i> Outcome of non-compliant, minor technical issues is due to operational issues identified by the agency to be resolved.</p>	

## Information provided to Ministry of Health

### 16 BDM (Births)/MoH NHI and Mortality Register

To verify and update information on the National Health Index and to compile mortality statistics.

*Births, Deaths, Marriages, and Relationships Registration Act 2021 s 112*

BDM disclosure to Ministry of Health (MoH): BDM provides child's names, gender, date of birth, place of birth, ethnicity, and parents' names, occupations, date of birth, place of birth, address(es) and ethnicities. BDM also indicates whether the baby was stillborn.



### 17 BDM (Deaths)/MoH NHI and Mortality Register

To verify and update information on the NHI and to compile mortality statistics.

*Births, Deaths, Marriages, and Relationships Registration Act 2021 s 112*

BDM disclosure to MoH: BDM provides full name (including name at birth if different from current name), address, occupation, ethnicity and gender, date and place of birth, date and place of death, and cause(s) of death.





## Information provided to Ministry of Justice

### 18 Customs/Justice Fines Defaulters Alerts

To improve the enforcement of fines by identifying serious fines defaulters as they cross New Zealand borders, and to increase voluntary compliance through publicity about the programme targeted at travellers.

*Customs and Excise Act 2018, s 310*

Justice disclosure to Customs: Justice provides Customs with the full name, date of birth, gender and Justice unique identifier number of serious fines defaulters for inclusion on the 'silent alerts' or 'interception alerts' lists.

Customs disclosure to Justice: For each alert triggered, Customs supplies the full name, date of birth, gender, nationality and presented passport number, along with details about the intended or just completed travel.

*Note:* Last year's assessment returned an outcome of non-compliant due to an aspect of reporting which was no longer fit for purpose and has led to under-reporting. This has now been resolved with the implementation of a new reporting system.



### 19 MSD/Justice Fines Defaulters Tracing

To enable the Ministry of Justice to locate people who have outstanding fines to enforce payment.

*Social Security Act 2018, Schedule 6, cl 13*

Justice disclosure to MSD: Justice selects fines defaulters for whom it has been unable to find a current address from other sources (including the IR/Justice Fines Defaulters Tracing Programme), and sends the full name, date of birth and data matching reference number to MSD.

MSD disclosure to Justice: For matched records, MSD returns the last known residential address, postal address, residential, mobile and work phone numbers, and the unique identifier originally provided by Justice.



### 20 IR/Justice Fines Defaulters Tracing

To enable the Ministry of Justice to locate people who have outstanding fines to enforce payment.

*Tax Administration Act 1994, Schedule 7 Part C subpart 2 cl 43*

Justice disclosure to IR: Justice selects fines defaulters for whom it has been unable to find a current address, and sends the full name, date of birth, and a data matching reference number to IR.

IR disclosure to Justice: For matched records, IR supplies the current address and all known telephone numbers for the person, the name, address, and contact numbers of the person's employer or employers, and the unique identifier originally provided by Justice.



## Information provided to Ministry of Social Development

### 21 ACC/MSD Benefit Eligibility

To identify individuals whose Ministry of Social Development (MSD) entitlement may have changed because they are receiving ACC payments, and to assist MSD in the recovery of outstanding debts.

*Accident Compensation Act 2001, s 281*

ACC disclosure to MSD: ACC selects individuals who have either:

- claims where there has been no payment made to the claimant for six weeks (in case MSD needs to adjust its payments to make up any shortfall)
- current claims that have continued for two months since the first payment, or
- current claims that have continued for one year since the first payment.

For these people, ACC provides MSD with the full name (including aliases), date of birth, address, IR number, ACC claimant identifier, payment start/end dates and payment amounts.



### 22 BDM/MSD Identity Verification

To confirm the validity of birth certificates used by clients when applying for financial assistance, and to verify that clients are not on the NZ Deaths Register.

BDM disclosure to MSD: BDM provides birth and death information for the 90 years prior to the extraction date.

*Births, Deaths, Marriages, and Relationships Registration Act 2021 s 112*

The birth details include the full name, gender, date of birth and place of birth, birth registration number and full name of both mother and father. The death details include the full name, gender, date of birth, date of death, home address, death registration number and spouse's full name.



### 23 BDM (Deaths)/MSD Deceased Persons

To identify current clients who have died so that MSD can stop making payments in a timely manner.

*Births, Deaths, Marriages, and Relationships Registration Act 2021 s 112*

BDM disclosure to MSD: BDM provides death information for the week prior to the extraction date. The death details include the full name, gender, date of birth, date of death, home address, death registration number and spouse's full name.







### 24 BDM (Marriages)/MSD Married Persons Benefit Eligibility




To identify current clients who have married so that MSD can update client records and reassess their eligibility for benefits and allowances.




*Births, Deaths, Marriages, and Relationships Registration Act 2021 s 112*




BDM disclosure to MSD: BDM provides marriage information covering the week prior to the extraction date. The marriage details include the full names of each spouse (including name at birth if different from current name), their date of birth and addresses, and registration and marriage dates.






25	<b>BDM/MSD Overseas Born Name Change</b>	
	<p>To verify a client's eligibility or continuing eligibility to a benefit where a client has legally changed their name in New Zealand and not informed MSD. The programme is also used to identify debtors and suspected benefit fraud.</p> <p><i>Births, Deaths, Marriages, and Relationships Registration Act 2021 s 112</i></p> <p>BDM provides name change records from January 2009 to the extract date. The name change details include the full name at birth, former full name, new full name, birth date, residential address, and country of birth.</p>	
26	<b>Corrections/MSD Prisoners</b>	
	<p>To detect people who are receiving income support payments while imprisoned, and to assist MSD in the recovery of outstanding debts.</p> <p><i>Corrections Act 2004, s 180</i></p> <p>Corrections disclosure to MSD: Each day, Corrections sends MSD details about all prisoners who are admitted, on muster or released from prison. Details disclosed include the full name (including aliases), date of birth, prisoner unique identifier and prison location, along with incarceration date, parole eligibility date and statutory release date.</p>	
27	<b>MoE/MSD (Study Link) Results of Study</b>	
	<p>To determine eligibility for student loans and/or allowance by verifying students' study results.</p> <p><i>Education and Training Act 2020, schedule 9 cl 7</i></p> <p>MSD StudyLink disclosure to Ministry of Education (MoE): StudyLink provides MoE with the student's name(s) (in abbreviated form), date of birth, IR number, first known study start date, end date (date of request), known education provider(s) used by this student and student ID number.</p> <p>MoE disclosure to MSD StudyLink: MoE returns to StudyLink information showing all providers and courses used by the student, course dates, course equivalent full-time student rating and course completion code.</p>	
28	<b>Educational Institutions/MSD (Study Link) Loans and Allowances</b>	
	<p>To verify student enrolment information to confirm entitlement to allowances and loans.</p> <p><i>Education and Training Act 2020, schedule 9 cl 8 &amp; 9</i></p> <p>MSD StudyLink disclosure to educational institutions: When requesting verification of student course enrolments, MSD StudyLink provides the educational institution the student's full name, date of birth, MSD client number and student ID number.</p> <p>Educational institutions' disclosure to MSD StudyLink: The educational institutions return to MSD StudyLink the student's enrolled name, date of birth, MSD client number, student ID number and study details.</p>	

<p><b>29</b></p>	<p><b>Justice/MSD Warrants to Arrest</b></p> <p>To enable MSD to suspend or reduce the benefits of people who have an outstanding warrant to arrest for criminal proceedings.</p> <p><i>Social Security Act 2018, Schedule 6, cl 15</i></p> <p>Justice disclosure to MSD: Justice provides MSD with the full name (and alias details), date of birth, address, Justice unique identifier and warrant to arrest details.</p>	
<p><b>30</b></p>	<p><b>Australia (Centrelink)/MSD Change in Circumstances</b></p> <p>For MSD and Centrelink (the Australian Government agency administering social welfare payments) to exchange benefit and pension applications, and changes of client information.</p> <p><i>Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Australia) Order 2017</i></p> <p>Centrelink disclosure to MSD: When Australian social welfare records are updated for people noted as having New Zealand social welfare records, Centrelink automatically sends an update to MSD including the full name, marital status, address, bank account, benefit status, residency status, income change, MSD client number and Australian Customer Reference Number.</p> <p>MSD disclosure to Centrelink: MSD automatically sends the same fields of information to Centrelink when New Zealand social welfare records are updated, if the person is noted as having an Australian social welfare record.</p>	
<p><b>31</b></p>	<p><b>Canada/MSD Social Welfare Reciprocity</b></p> <p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and Canada.</p> <p><i>Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Canada) Order 1996</i></p> <p>Canada disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information and Social Security numbers.</p> <p>MSD disclosure to Canada: includes full name, date of birth, marital status, address, entitlement information and MSD client number.</p> <p><i>Note:</i> Non-compliant – minor technical issues rating is due to MSD yet to confirm that they fixed the notice of Information Matching letter advising of process around changes to entitlement not sent, but adverse action letters advising of actual changes are sent.</p>	

32	<p><b>Denmark/MSD Social Welfare Reciprocity</b></p> <p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and Denmark.</p> <p><i>Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Denmark) Order 1997</i></p> <p>Denmark disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information and Social Security numbers.</p> <p>MSD disclosure to Denmark: includes full name, date of birth, marital status, address, entitlement information and MSD client number.</p> <p><i>Note:</i> Non-compliant – minor technical issues rating is because MSD has yet to confirm the ongoing resolution regarding notice of Information Matching letter advising of process around changes to entitlements.</p>	
33	<p><b>Hellenic Republic/MSD Social Welfare Reciprocity</b></p> <p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and the Hellenic Republic.</p> <p><i>Social Security Act 2018, s 380 and Social Welfare (Reciprocity with the Hellenic Republic) Order 1993</i></p> <p>Hellenic Republic disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information and Social Security numbers.</p> <p>MSD disclosure to Hellenic Republic: includes full name, date of birth, marital status, address, entitlement information and MSD client number.</p> <p><i>Note:</i> Non-compliant – minor technical issues rating is due to MSD yet to confirm resolution to the gaps identified in the notice of Information Matching letter advising of process around changes to entitlement not sent.</p>	
34	<p><b>Ireland/MSD Social Welfare Reciprocity</b></p> <p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and Ireland.</p> <p><i>Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Ireland) Order 1993</i></p> <p><i>Ireland disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information and Social Security numbers.</i></p> <p>MSD disclosure to Ireland: includes full name, date of birth, marital status, address, entitlement information and MSD client number.</p> <p><i>Note:</i> Non-compliant – minor technical issues rating is due to MSD yet to confirm resolution to the gaps identified in the notice of Information Matching letter advising of process around changes to entitlement not sent.</p>	

35	<b>Jersey and Guernsey/MSD Social Welfare Reciprocity</b>	
<p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and Jersey and Guernsey.</p> <p><i>Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Jersey and Guernsey) Order 1995</i></p> <p>Jersey and Guernsey disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information and Social Security numbers.</p> <p>MSD disclosure to Jersey and Guernsey: includes full name, date of birth, marital status, address, entitlement information and MSD client number.</p> <p><i>Note:</i> Non-compliant – minor technical issues rating is due to MSD yet to confirm resolution to the gaps identified in the notice of Information Matching letter advising of process around changes to entitlement not sent.</p>		
36	<b>Malta/MSD Social Welfare Reciprocity</b>	
<p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and Malta.</p> <p><i>Social Security Act 2018, s 380; Social Welfare (Reciprocity with Malta) Order 2013</i></p> <p>Malta disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information and Maltese Identity Card and Social Security numbers.</p> <p>MSD disclosure to Malta: includes full name, date of birth, marital status, address, entitlement information and MSD client number.</p>		
37	<b>Netherlands/MSD Change in Circumstances</b>	
<p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and the Netherlands.</p> <p><i>Social Security Act 2018, s 380 and Social Welfare (Reciprocity with the Netherlands) Order 2003</i></p> <p>MSD disclosure to Netherlands: MSD forwards the appropriate application forms to the Netherlands Sociale Verzekeringsbank (SVB). The forms include details such as the full names, dates of birth, addresses and MSD client number.</p> <p>Netherlands disclosure to MSD: SVB responds with the SVB reference number.</p>		

38	<b>Netherlands/MSD General Adjustment</b>	
<p>To enable the processing of general adjustments to benefit rates for individuals receiving pensions from both New Zealand and the Netherlands.</p> <p><i>Social Security Act 2018, s 380 and Social Welfare (Reciprocity with the Netherlands) Order 2003</i></p> <p>MSD disclosure to Netherlands: For MSD clients in receipt of both New Zealand and Netherlands pensions, MSD provides the Netherlands Sociale Verzekeringsbank (SVB) with the changed superannuation payment information, the MSD client reference number and the Netherlands unique identifier.</p> <p>Netherlands disclosure to MSD: SVB advises adjustments to payment rates and the 'holiday pay' bonus.</p>		
39	<b>South Korea/MSD Social Welfare Reciprocity</b>	
<p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and the Republic of Korea (South Korea).</p> <p><i>Social Security Act 2018, s.380 and Social Security (Reciprocity with the Republic of Korea) Order 2021</i></p> <p>South Korea disclosure to MSD: includes full name, date of birth, marital status, address, entitlement information and Korean National Pension Number (or Korean Resident Registration Number).</p> <p>MSD disclosure to South Korea: includes full name, date of birth, marital status, address, entitlement information and New Zealand Client Number.</p>		
40	<b>United Kingdom/MSD Social Welfare Reciprocity</b>	
<p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and the United Kingdom.</p> <p><i>Social Security Act 2018, s.380 and Social Security (Reciprocity with the United Kingdom) Order 1990</i></p> <p>UK disclosure to MSD: includes full name, date of birth, marital status, address, entitlement information and Social Security numbers.</p> <p>MSD disclosure to UK: includes full name, date of birth, marital status, address, entitlement information and New Zealand Client Number.</p> <p><i>Note:</i> Non-compliant – minor technical issues rating is due to MSD yet to confirm resolution to the gaps identified in the notice of Information Matching letter advising of process around changes to entitlement not sent.</p>		



## Information provided to Teaching Council of New Zealand

### 41 MoE/Teaching Council Registration

To ensure teachers are correctly registered (Teaching Council) and paid correctly (Ministry of Education).

*Education and Training Act 2020, schedule 3 cl 9*

MoE disclosure to Teaching Council: MoE provides full name, date of birth, gender, address, school(s) employed at, number of half days worked, registration number (if known), and MoE employee number.

Teaching Council disclosure to MoE: The Teaching Council provides full name, date of birth, gender, address, registration number, registration expiry date, registration classification and MoE employee number (if confirmed).



## Information provided to NZTA Waka Kotahi

### 42 BDM (Deaths)/NZTA Deceased Driver License Holders

To improve the quality and integrity of data held on the Driver License Register by identifying license holders who have died.

*Births, Deaths, Marriages, and Relationships Registration Act 2021 s 112*

BDM disclosure to New Zealand Transport Agency (NZTA): BDM provides death information for the fortnight prior to the extraction date. The death details include the full name (including name at birth if different from current name), gender, date and place of birth, date of death, home address and death registration number.



### INDEPENDENT AUDITOR'S REPORT TO THE READERS OF THE PRIVACY COMMISSIONER'S ANNUAL FINANCIAL STATEMENTS AND PERFORMANCE INFORMATION FOR THE YEAR ENDED 30 JUNE 2025

The Auditor-General is the auditor of the Privacy Commissioner. The Auditor-General has appointed me, Bryce Henderson, using the staff and resources of Deloitte Limited, to carry out, on his behalf, the audit of:

- the annual financial statements that comprise the statement of financial position as at 30 June 2025, the statement of comprehensive revenue and expenses, statement of changes in equity, and statement of cash flows for the year ended on that date and the notes to the financial statements that include accounting policies and other explanatory information on pages 55 to 70; and
- the performance information that consists of:
  - the statement of performance for the year ended 30 June 2025 on pages 50 to 54; and
  - the end-of-year performance information for appropriations for the year ended 30 June 2025 on pages 47 to 54.

#### Opinion

In our opinion:

- The annual financial statements of the Privacy Commissioner:
  - fairly present, in all material respects:
    - its financial position as at 30 June 2025; and
    - its financial performance and cash flows for the year then ended; and
  - comply with generally accepted accounting practice in New Zealand in accordance with with the Public Benefit Entity Standards Reduced Disclosure Regime; and
- The statement of performance fairly presents, in all material respects, the Privacy Commissioner's performance for the year ended 30 June 2025. In particular, the statement of performance:
  - provides an appropriate and meaningful basis to enable readers to assess the actual performance of the Privacy Commissioner for each class of reportable outputs; determined in accordance with generally accepted accounting practice in New Zealand; and
  - fairly presents, in all material respects, for each class of reportable outputs:
    - the actual performance of the Privacy Commissioner;
    - the actual revenue earned; and

- the output expenses incurred

as compared with the forecast standards of performance, the expected revenues, and the proposed output expenses included in the Privacy Commissioner's statement of performance expectations for the financial year; and

- complies with generally accepted accounting practice in New Zealand in accordance with the Public Benefit Entity Standards Reduced Disclosure Regime.
- The end-of-year performance information for appropriations:
  - provides an appropriate and meaningful basis to enable readers to assess what has been achieved with the appropriation; determined in accordance with generally accepted accounting practice in New Zealand; and
  - fairly presents, in all material respects:
    - what has been achieved with the appropriation; and
    - the actual expenses or capital expenditure incurred in relation to the appropriation as compared with the expenses or capital expenditure that were appropriated or forecast to be incurred; and
  - complies with generally accepted accounting practice in New Zealand in accordance with the Public Benefit Entity Standards Reduced Disclosure Regime.

Our audit was completed on 24 October 2025. This is the date at which our opinion is expressed.

### **Basis for our opinion**

We carried out our audit in accordance with the Auditor-General's Auditing Standards, which incorporate the Professional and Ethical Standards, the International Standards on Auditing (New Zealand), and New Zealand Auditing Standard 1 (Revised): *The Audit of Service Performance Information* issued by the New Zealand Auditing and Assurance Standards Board. Our responsibilities under those standards are further described in the *Responsibilities of the auditor* section of our report.

We have fulfilled our responsibilities in accordance with the Auditor-General's Auditing Standards.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

### **Responsibilities of the Privacy Commissioner for the annual financial statements and performance information**

The Privacy Commissioner is responsible on behalf of the Privacy Commissioner for preparing:

- Annual financial statements that fairly present the Privacy Commissioner's financial position, financial performance, and its cash flows, and that comply with generally accepted accounting practice in New Zealand.

- A statement of performance that:
  - provides an appropriate and meaningful basis to enable readers to assess the actual performance of the Privacy Commissioner for each class of reportable outputs; determined in accordance with generally accepted accounting practice in New Zealand;
  - fairly presents, for each class of reportable outputs:
    - the actual performance of the Privacy Commissioner;
    - the actual revenue earned; and
    - the output expenses incurred

as compared with the forecast standards of performance, the expected revenues, and the proposed output expenses included in the Privacy Commissioner's statement of performance expectations for the financial year; and

  - complies with generally accepted accounting practice in New Zealand.
- End-of-year performance information for appropriations that:
  - provides an appropriate and meaningful basis to enable readers to assess what has been achieved with the appropriation; determined in accordance with generally accepted accounting practice in New Zealand;
  - fairly presents what has been achieved with the appropriation;
  - fairly presents the actual expenses or capital expenditure incurred in relation to the appropriation as compared with the expenses or capital expenditure that were appropriated or forecast to be incurred; and
  - complies with generally accepted accounting practice in New Zealand.

The Privacy Commissioner is responsible for such internal control as they determine are necessary to enable them to prepare annual financial statements, and the performance information that are free from material misstatement, whether due to fraud or error.

In preparing the annual financial statements, and performance information, the Privacy Commissioner is responsible on behalf of the Privacy Commissioner for assessing the Privacy Commissioner's ability to continue as a going concern.

The Privacy Commissioner's responsibilities arise from the Crown Entities Act 2004 and the Public Finance Act 1989.

## **Responsibilities of the auditor for the audit of the annual financial statements and performance information**

Our objectives are to obtain reasonable assurance about whether the annual financial statements, the statement of performance, and the end-of-year performance information for appropriations, as a whole, are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion.

Reasonable assurance is a high level of assurance, but is not a guarantee that an audit carried out in accordance with the Auditor-General's Auditing Standards will always detect a material

misstatement when it exists. Misstatements are differences or omissions of amounts or disclosures, and can arise from fraud or error. Misstatements are considered material if, individually or in the aggregate, they could reasonably be expected to influence the decisions of readers, taken on the basis of the annual financial statements, and the statement of performance, and the end-of-year performance information for appropriations.

For the budget information reported in the annual financial statements, and the statement of performance, and the end-of-year performance information for appropriations, our procedures were limited to checking that the information agreed to the Privacy Commissioner's statement of performance expectations or to the Estimates of Appropriations for the Government of New Zealand for the Year Ending 30 June 2025.

We did not evaluate the security and controls over the electronic publication of the annual financial statements, and the statement of performance, and the end-of-year performance information for appropriations.

As part of an audit in accordance with the Auditor-General's Auditing Standards, we exercise professional judgement and maintain professional scepticism throughout the audit. Also:

- We identify and assess the risks of material misstatement of the annual financial statements, the statement of performance, and the end-of-year performance information for appropriations, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control
- We obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Privacy Commissioner's internal control.
- We evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by the Privacy Commissioner.
- We evaluate whether the statement of performance and the end-of-year performance information for appropriations:
  - provide an appropriate and meaningful basis to enable readers to assess the actual performance of the Privacy Commissioner in relation to the actual performance of the Privacy Commissioner (for the statement of performance) and what has been achieved with the appropriation by the Privacy Commissioner (for the end-of-year performance information for appropriations). We make our evaluation by reference to generally accepted accounting practice in New Zealand; and
  - fairly present the actual performance of the Privacy Commissioner and what has been achieved with the appropriation by the Privacy Commissioner for the financial year.
- We conclude on the appropriateness of the use of the going concern basis of accounting by the Privacy Commissioner.

- We evaluate the overall presentation, structure and content of the annual financial statements, the statement of performance, and the end-of-year performance information for appropriations, including the disclosures, and whether the annual financial statements, the statement of performance, and the end-of-year performance information for appropriations represent the underlying transactions and events in a manner that achieves fair presentation.

We communicate with the Privacy Commissioner regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that we identify during our audit.

Our responsibilities arise from the Public Audit Act 2001.

## Other information

The Privacy Commissioner is responsible for the other information. The other information comprises all of the information included in the annual report, but does not include the annual financial statements, the statement of performance, and the end-of-year performance information for appropriations, and our auditor's report thereon.

Our opinion on the annual financial statements, and the statement of performance, and the end-of-year performance information for appropriations, does not cover the other information and we do not express any form of audit opinion or assurance conclusion thereon.

In connection with our audit of the annual financial statements, and the statement of performance, and the end-of-year performance information for appropriations, our responsibility is to read the other information. In doing so, we consider whether the other information is materially inconsistent with the annual financial statements, and the statement of performance, and the end-of-year performance information for appropriations or our knowledge obtained in the audit, or otherwise appears to be materially misstated. If, based on our work, we conclude that there is a material misstatement of this other information, we are required to report that fact. We have nothing to report in this regard.

## Independence

We are independent of the Privacy Commissioner in accordance with the independence requirements of the Auditor-General's Auditing Standards, which incorporate the independence requirements of Professional and Ethical Standard 1: *International Code of Ethics for Assurance Practitioners (including International Independence Standards)* (New Zealand) issued by the New Zealand Auditing and Assurance Standards Board.

Other than in our capacity as auditor, we have no relationship with, or interests in, the Privacy Commissioner.



Bryce Henderson  
**Deloitte Limited**  
**On behalf of the Auditor-General**  
Auckland, New Zealand







Privacy Commissioner  
Te Mana Mātāpono Matatapu

ISSN 1179-9838 (Print)  
ISSN 1179-9846 (Online)