

PRIVACY COMMISSIONER

Annual Report 2022



Annual Report of the Privacy Commissioner

for the year ended 30 June 2022

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

The Minister of Justice

I tender my report as Privacy Commissioner for the year ended 30 June 2022

A handwritten signature in black ink that reads "Michael Webster". The signature is written in a cursive style with a long horizontal stroke at the end.

Michael Webster
Privacy Commissioner
31 March 2023

Introduction Kupu Whakataki	2
Privacy in Aotearoa New Zealand – the year in numbers Te Mana Matatapu i Aotearoa – te tau me ōna tino tau	4
Strategic objectives progress Te kauneke ki ngā whāinga rautaki	6
Objective 1: Privacy protection is effective and easy to achieve	6
Objective 2: Costs of privacy compliance are minimised	9
Objective 3: We are trusted as a fair and responsive regulator	13
Objective 4: We influence privacy practices and behaviour	17
Office and functions Te Tari me āna mahi	20
Independence and competing interests	21
Reporting	21
Staff	22
COVID-19	22
Statutory remuneration disclosures	23
EEO profile	24
Finance and performance report Pūrongo whakahaere pūtea me ngā tutukitanga	26
Statement of responsibility	27
Statement of performance	28
Impact of the COVID-19 emergency on performance	28
PBE FRS 48 service performance reporting	29
Statement specifying comprehensive income	29
Cost of service statement for the year ended 30 June 2022	30
Primary activity 1: Strategy and insights	32
Primary activity 2: Communications and education	33
Primary activity 3: Compliance and enforcement	34
Primary activity 4: Advice and advocacy	35
Primary activity 5: Investigations and dispute resolution	36
Statement of accounting policies	37
Statement of comprehensive revenue and expenses	39
Statement of changes in equity	40
Statement of financial position	41
Statement of cash flows	42
Notes to the financial statements	43
Appendices Ngā Tāpiritanga	58
Appendix A Processes and services	59
Appendix B Information matching 2021/22	61
Appendix C Independent Auditor’s Report	76

Introduction | Kupu Whakataki

Titiro whakamuri, te haere whakamua

E ngā mana, e ngā reo, e ngā rau Rangatira, tēnā koutou, tēnā koutou, tēnā tātou katoa.

As I look back on the past year, I first want to acknowledge the previous Privacy Commissioner, John Edwards, and former Acting Privacy Commissioner, Liz MacPherson. Their groundwork has enabled us to extend our influence for improved privacy practice across Aotearoa New Zealand over the past year.

Captured by the whakataukī above, we are best placed to face the future when we understand the past.

I am mindful of the journey this office has navigated as the COVID-19 pandemic shaped and influenced our work programme. There is a consistent theme of our people working together to achieve better privacy outcomes in the face of extraordinary challenges.

In last year's Annual Report, we highlighted the launch of the Privacy Act 2020 and the powers that would better enable us to effectively regulate how organisations and businesses collect, store, use and share people's personal information. Since then, the Office has developed a new strategic framework and outcomes, and new tools to make privacy easier for organisations.

This year, we devoted a significant amount of resource toward supporting Aotearoa New Zealand's response to COVID-19, ensuring privacy was kept front-of-mind during major developments including workforce vaccination rules.

We released a position paper on how the Privacy Act regulates biometric information, to improve understanding of the privacy considerations when collecting and using this form of sensitive personal information.



In this reporting period we were also able to deliver on our key strategic priorities including:

- Working with key stakeholders from both sides of the rental market to develop guidance for tenants, landlords, and others to understand their privacy rights. We set out what information may be requested at every stage of the rental process, and developed and launched a compliance framework.
- We supported numerous organisations across various sectors to better understand their obligation to allow people to access personal information held about them.
- Our staff and partners hosted 15 webinars across Privacy Week 2022, Privacy: The Foundation of Trust. We covered a broad range of topics aimed at sharing good privacy practice for organisations including privacy in schools and the health sector.
- Our strategic focus on embedding Te Ao Māori perspectives in our work saw us host our first public tikanga and privacy webinar, *Tikanga Māori and Privacy: Reflections from the High Court review of decisions about Māori COVID-19 vaccination data*, as part of Privacy Week 2022.

It is thanks to the commitment of our people, and those we work with, that we have been able to make this progress as we continue to advocate for the personal information of all New Zealanders to be respected and protected, by the organisations and institutions that hold and use this precious taonga. I look forward to continuing our efforts to promote individual privacy in the coming year as we near the thirtieth anniversary of the original Privacy Act 1993.

Nō reira e tika ana te kōrero titiro whakamuri, te haere whakamua.

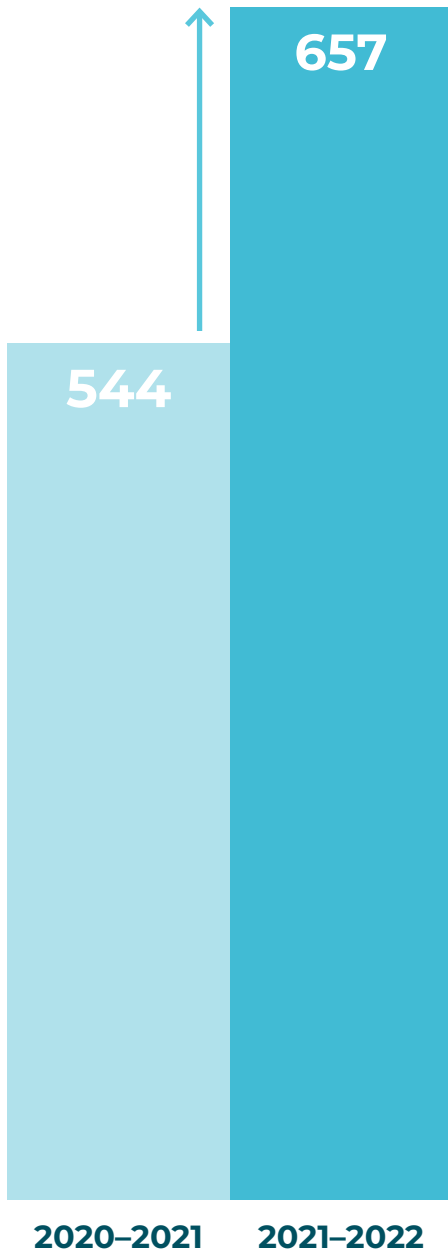
Michael Webster
Privacy Commissioner

This year, we devoted a significant amount of resource toward supporting Aotearoa New Zealand's response to COVID-19, ensuring privacy was kept front-of-mind.



Privacy in Aotearoa New Zealand – the year in numbers | Te Mana Matatapu i Aotearoa – te tau me ōna tino tau

Number of privacy breach notifications



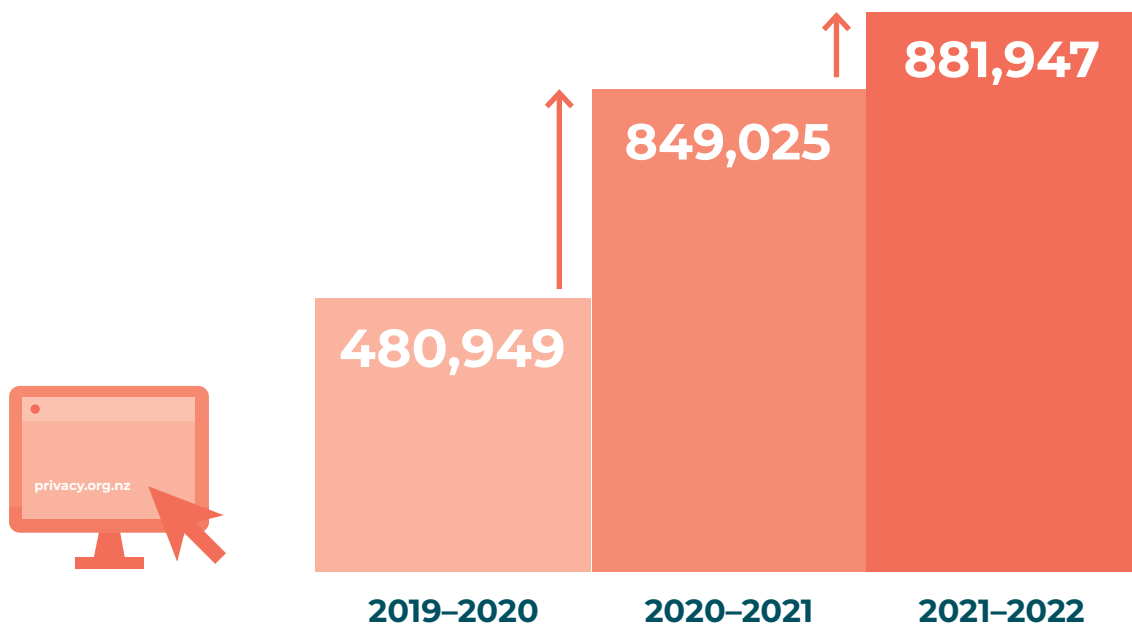


7,586
enquiries received



184
media enquiries received

Visits to our website



Strategic objectives progress | Te kauneke ki ngā whāinga rautaki



Objective 1 | Whāinga 1 Privacy protection is effective and easy to achieve He whaikiko he māmā hoki te tutuki i te tiakitanga matatapu

Effective privacy protection means people can feel confident in the knowledge that organisations trusted with their personal information are equipped to safeguard it from harm.

This year, we have continued improving our services to ensure effective privacy protection is as easy as possible for organisations to achieve, providing advice on compliance with the Privacy Act and informing people of their rights to information about how organisations use their personal information.

We continue to provide free advice for organisations through our website, social media, newsletters, and enquiries service, enabling them to manage personal information in privacy-enhancing ways. We made the most of opportunities to educate organisations that the Privacy Act provides people with the right to access personal information held about them in a timely manner, connecting with and presenting to more than 50 organisations and entities throughout the year.

A strategic focus remains improving people's ability to access their own information. Issues relating to this right of access represent approximately 20% of enquiries we receive and more than 60% of the privacy complaints we investigate.

We are continuously developing our services to ensure people can engage in society knowing their privacy interests are being protected, and that we provide services if things go wrong. As an Office, we have continued to build our cultural capabilities and engage with tangata whenua to understand how we can best support their privacy aspirations. We now have a principal Māori advisor position, to support a strategic focus on embedding Te Ao Māori perspectives in our work. A highlight for us was hosting our first public tikanga and privacy webinar, *Tikanga Māori and Privacy: Reflections from the High Court review of decisions about Māori COVID-19 vaccination data*, as part of Privacy Week 2022.

Our Investigations and Dispute Resolution Team has used conciliation conferences as a way of increasing efficiency and effectiveness. We have held at least 10 settlement conferences over the past year – including our first hui hohou i te rongo, a whānau conciliation conference based in tikanga Māori.

CASE STUDY

Conciliation hui helps settle health information breach

A woman complained on behalf of her elderly father that a hospital had incorrectly recorded he had a history of cancer. The incorrect information was subsequently released to another agency, which later used it in a report sent to the father.

Consequently, the man worried that he had cancer, and no-one had told him. The hospital apologised and corrected the error after the man's distressed whānau queried the false health information held by the other agency.

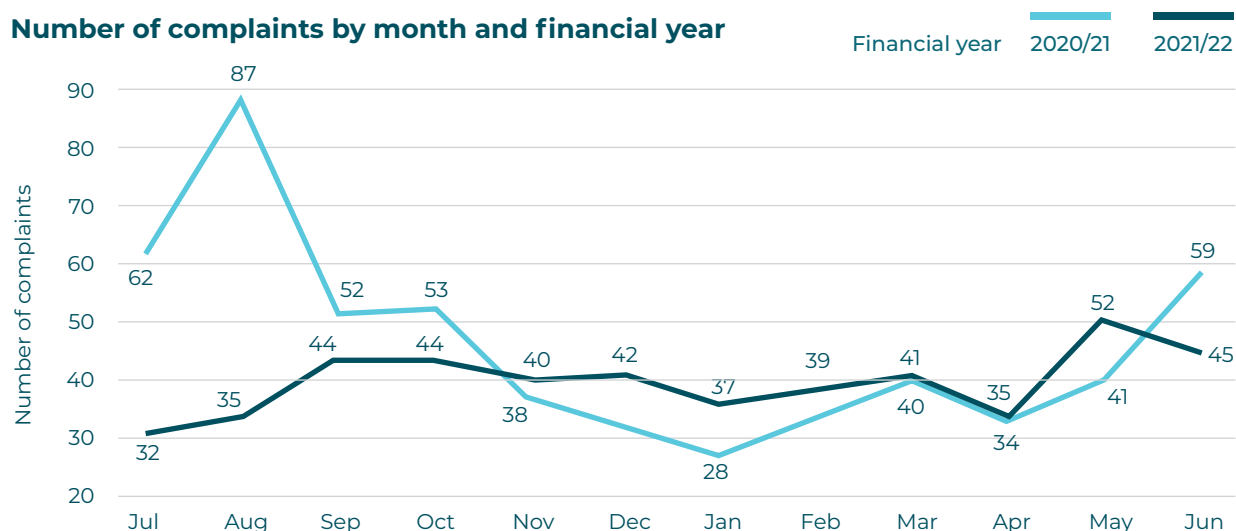
The man's daughter complained to us on his behalf, speaking of the ongoing emotional damage caused by the error, including how the mana and tapu of her father and whānau had been hurt.

While the hospital had apologised for the error and conducted a review to help ensure it did not happen again, the woman sought an independent investigation plus compensation. She requested a hui hohou i te rongo, a conciliatory meeting, to help her father and the whānau restore their mana.

The hospital had already completed its investigation and had accepted it had breached the man's privacy, so we advised the hospital that we wanted to explore a settlement without investigation by facilitating a hui at the request of the whānau. The hospital advised it was happy to participate in this process.

With the support of tikanga Māori expertise from our staff, the whānau and the hospital, we helped facilitate a hui hohou i te rongo for the first time.

The hui began with a mihi whakatau and incorporated karakia and waiata. The whānau also brought a manea stone to support kai kōrero and kai manaaki while people spoke. In this case, we were able to ensure the parties came together kanohi ki te kanohi/face to face and ensure a resolution that the whānau felt restored and protected their mana.

Number of complaints by month and financial year

CASE STUDY

Complaint self-assessment online tool success

Over the past year, OPC sought to improve the efficiency and timeliness of our management of people's privacy complaints, by improving our triaging of complaints and enquiries.

We introduced a new online complaint self-assessment tool, stepping people through whether their complaint is one we can investigate or if there is any action they need to take first. Each question refines the person's query, providing detail that will ultimately determine whether their issue falls under the Privacy Act or is better steered toward a different resolution.

This year, we also established an advisor, assessment and resolution position to help triage complaints and identify files that can be resolved early or do not warrant investigation.

We have experienced a reduction in the number of people's privacy complaints to be investigated, and believe this is due to simpler complaints being resolved more quickly, either through the intervention of the new Advisor role, or through our new online tools which make it easier for people to take action on their own behalf.



We introduced a new online complaint self-assessment tool stepping people through whether their complaint is one we can investigate or if there is any action they need to take first.



Objective 2 | Whāinga 2

Costs of privacy compliance are minimised

Ka whakahekea ngā utu mō te whakaū matatapu

By enabling organisations to reach levels of privacy maturity, we help them to identify ways to manage their collection and use of people’s personal information and comply with the Privacy Act.

An advantage of the Act is its ability to enable the flow of personal information where necessary for lawful purposes and objectives. Organisations can incorporate privacy protection as part of technological or other system improvements using “privacy by design”.

Our tools and processes help agencies prioritise privacy as a foundation of good practice, including providing detailed guidance for agencies to develop their own Privacy Impact Assessments for new projects, tools and technologies they may be considering.

We make it easy for organisations to upskill and develop their privacy capabilities through the provision of free online learning on a range of privacy topics from the basics to subject-specific. We also provide free educational opportunities for a broad range of sectors. Privacy Week 2022, *Privacy: The Foundation of Trust*, was a key opportunity for agencies to expand their privacy knowledge.

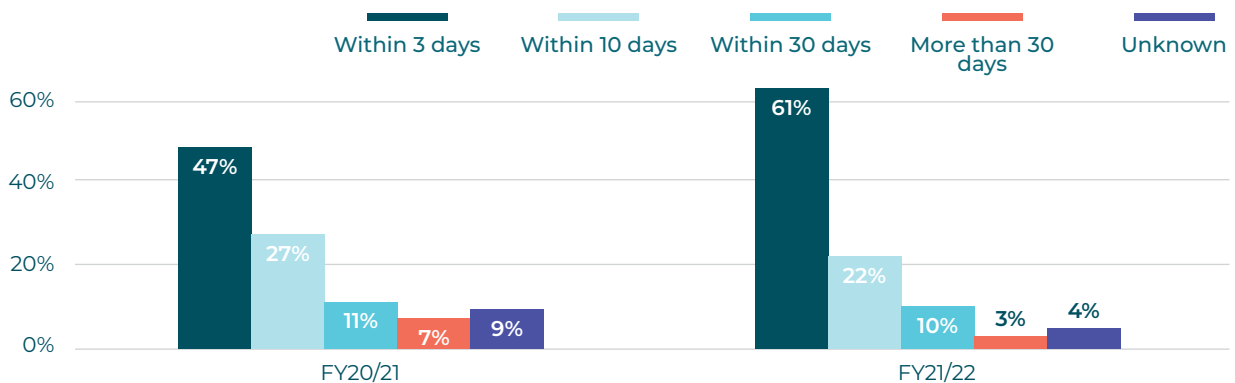
We provide advice to public and private sector organisations about complying with the Act and improving their responses to privacy harms.

Over the past year, a key focus has been encouraging agencies to report breaches within 72 hours. When a breach is notified, our Compliance Team seeks to swiftly triage and follow up with the agency concerned, providing advice and support as they work through the impacts of the breach on their organisation, team and customers or clients.

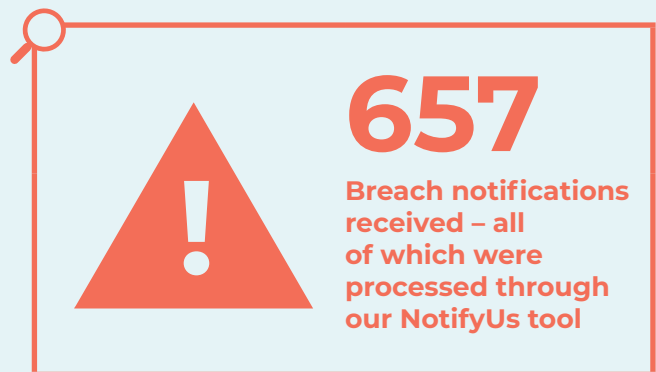
Privacy breaches are reported from the public, private and not for profit sectors and across a wide range of industries, with health care and social assistance reporting the highest number of privacy breaches.

While we have been receiving privacy breach notifications for over a decade, notifications initially jumped after becoming mandatory when the Privacy Act 2020 commenced in December 2020.

Timeliness of serious breach reporting to OPC

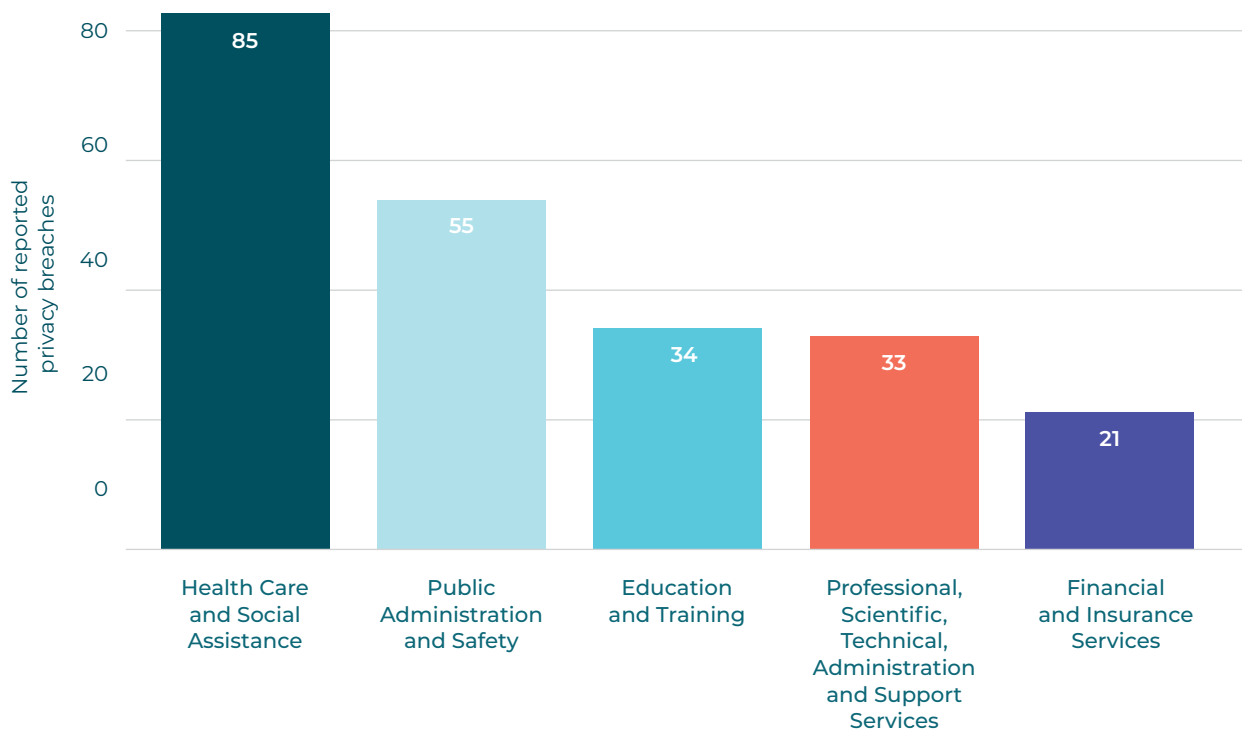


The volume of notified breaches have been fluctuating significantly since we saw a large increase following December 2020. In the last financial year, we received 657 breach notifications – all of which were processed through our NotifyUs tool which enables businesses and organisations to easily assess whether a privacy breach is notifiable. This was up from a total of 544 notifications the year before.



657
Breach notifications received – all of which were processed through our NotifyUs tool

Top five fields reporting serious privacy breaches



CASE STUDY**Waikato DHB cyber-attack**

In May 2021, the former Waikato District Health Board, now Te Whatu Ora Waikato, was hit by a major ransomware attack that impacted systems and services, causing delays to some medical care and support for vulnerable New Zealanders.

The former health board notified us within hours of becoming aware of the attack. This enabled us to act as a sounding board as they navigated their way through the many complex privacy implications of this significant attack including assessing how to approach the notification and support of affected individuals and communicate an evolving and uncertain situation to the public.

During this attack, hackers stole the personal information relating to various patients and staff, sending some data to media as 'proof' of the attack.

We quickly issued a media release, reminding everyone that it is vital for people to respect the personal information of others, and to treat the information as they would expect others to treat their own if it were disclosed.

Months later, the personal details of these individuals were disclosed on the dark web. Following RNZ reporting on personal information sourced from the dark web, the former health board obtained a High Court injunction to limit further access or disclosure of the illegally obtained information.

Our Compliance Team has continued to monitor the response to the attack. This has included understanding causes and getting assurances of appropriate remediation, including reviewing internal and external reports and being consulted by the independent review the Ministry of Health – Manatū Hauora commissioned.

CASE STUDY

Our free privacy e-learning courses continue to grow in popularity

First introduced in 2015, more than 25,000 e-learning modules had been completed by 2019. That number has now skyrocketed to more than 125,000 completed modules. While there was a significant spike in 2021 due to the introduction of the new Act, uptake of the modules has remained high with almost 40,000 completed in the past year, substantially higher than the comparable numbers for 2019/20.

Easy to follow, written in plain English and with real-world examples, these modules are a great way of growing people's knowledge of the Privacy Act.

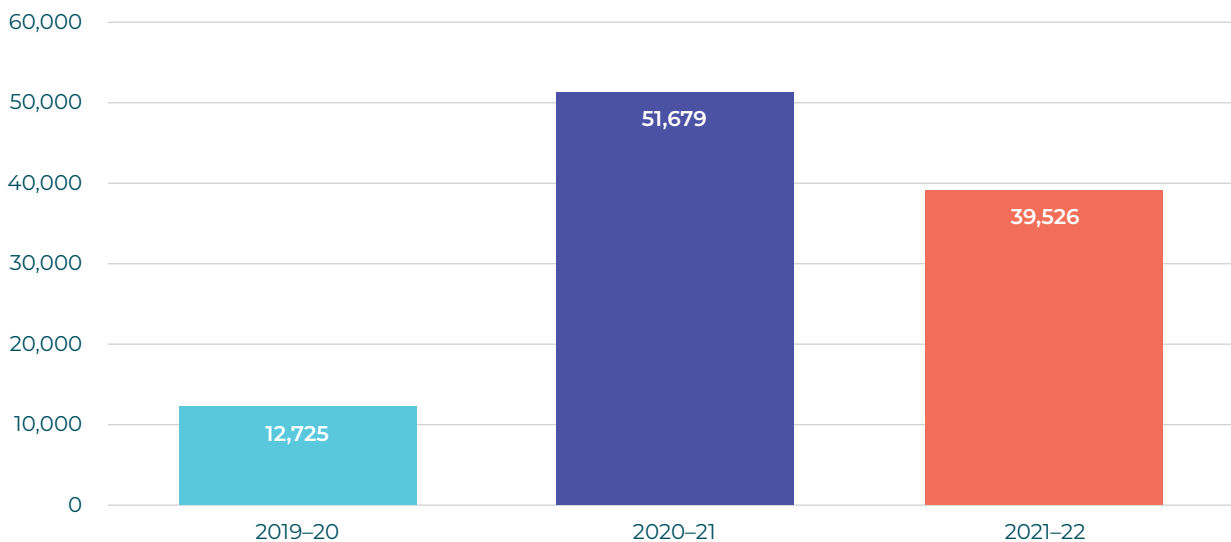
The most popular of these is Privacy ABC, which has been completed more than 29,000 times. Privacy ABC is short and to-the-point.

Using 11 scenarios, it gives users a quick and ready overview of some key privacy issues – and it takes less than half an hour to do so.

The second most popular module with more than 26,000 total completions is our Health ABC course. It provides a free 30-minute introduction to protecting health information under the Health Information Privacy Code. Our Health 101 course, which has been completed more than 12,000 times, goes a step further to introduce people to key concepts and definitions contained in the Health Information Privacy Code and how they may be applied in practice.

Other modules cover updates from the Privacy Act 2020, Privacy in Employment, and Privacy ABC for Schools.

E-learning completions by year





Objective 3 | Whāinga 3

We are trusted as a fair and responsive regulator

He meawhakawhirinaki mātou heikaiwhakarite tokeke, tika hoki

We aim to be trusted as a fair and responsive privacy regulator in Aotearoa New Zealand. Privacy is the foundation of trust, and we promote the importance of protecting it to organisations and the public.

Key to this work has been the values set out in our Compliance and Regulatory Action Framework (CARAF), which outlines how we approach our regulatory role. We set ourselves clear guiding principles including fairness, consistency and transparency, proportionality, accountability, and kōtuitui (seeking opportunities to partner with Māori whenever possible).

The CARAF outlines clear decision factors we would apply when considering action:

- seriousness or potential impact of a privacy issue on individuals
- the level of public interest in the issue
- the attitude to compliance and conduct of the agency concerned.

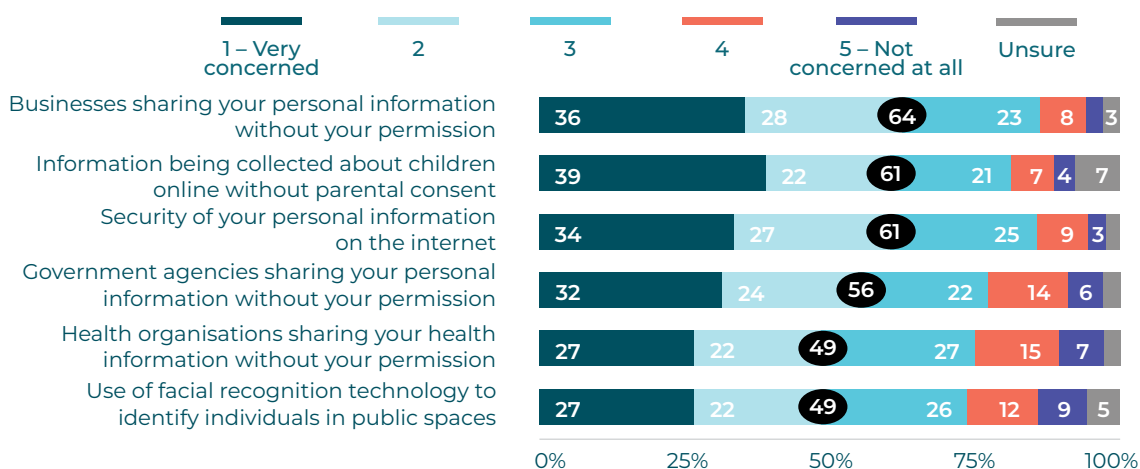
We have continued to highlight the need for organisations to see privacy protection as essential for earning trusting relationships. Over the past year, we have advised numerous organisations reporting serious breaches on how to minimise the harm that these breaches cause to people and learn from them so that they do not occur again.

Our March 2022 research into the privacy concerns of New Zealanders showed that more than half of New Zealanders are concerned about their personal information being shared by business and government, and that 7% of New Zealanders had been personally affected by a privacy breach in the past year.

It also revealed that three in five people would likely consider changing providers if they heard they had poor privacy and security practices. It means the care and protection of New Zealanders' personal information is critical to an agency's reputation.

Our March 2022 research into the privacy concerns of New Zealanders showed that more than half of New Zealanders are concerned about their personal information being shared.

How concerned are you about the following issues in New Zealand today? (%)



As a trusted regulator, it is essential for us to set clear expectations for agencies. Throughout the 2021/22 year we continued our work with the IPCA on the joint inquiry focused on Police practice of photographing members of the public who were not being detained or suspected of committing an offence.

The joint inquiry was announced in December 2020 following substantial media publicity about Police taking photographs of Māori young people in Wairarapa in August 2020. While the photographing of youth remains a key focus of the inquiry, the terms of reference were broadened to include the photographing of other members of the public. The final report was scheduled for release in September 2022.

Biometric information is uniquely sensitive to each of us. It is the biological and behavioural details that make us who we are – it can include our facial details, voice, fingerprints or even how we walk.

There is growing concern about how facial recognition technology and biometrics are regulated, and we have been exploring whether further regulatory intervention is required for its use in Aotearoa New Zealand.

In October 2021, we released a position paper on how the Privacy Act regulates biometrics. This paper informs decision-making about biometrics by agencies covered by the Privacy Act, in both the public and private sectors.

Using biometric technologies can have benefits for organisations, including convenience, efficiency, and security, but they can also create significant risks. These can include surveillance and profiling, lack of transparency and control, and accuracy, bias, and discrimination.

Our paper set out our approach to the regulation of biometrics under the Privacy Act and the expectations of agencies using or proposing to use biometrics. It also contributes to the ongoing discussion about whether existing regulatory frameworks adequately address the risks and maintain the benefits of using biometric technologies.

CASE STUDY

Issuing our first compliance notice

We can issue compliance notices to organisations or businesses that are not meeting their obligations under the Privacy Act. The notices detail changes the agency needs to make to its systems or processes to comply with the Act. Notices can also provide learnings for other opportunities about steps required for compliance with the Act.

In 2021, we issued the first compliance notice under the Privacy Act 2020. The notice was issued to the Reserve Bank of New Zealand – Te Pūtea Matua following the bank's response to a cyber-attack in December 2020.

The Reserve Bank was the victim of a cyber-attack which raised the possibility of systemic weaknesses in the Bank's systems and processes for protecting personal information. As a result, the Bank instigated an internal and external review to identify any shortcomings in their operations.

Following review of the privacy breach, the Privacy Commissioner determined that the Reserve Bank failed to adequately protect a subset of personal information it held despite security safeguards.

This compliance notice was issued to the Reserve Bank to improve their policies and procedures and make their systems more secure for handling personal information. The compliance notice targeted specific steps to be taken within identified timeframes and progress against this was monitored by the Office of the Privacy Commissioner.

The Reserve Bank instigated a programme of work to improve policies and processes for protecting personal information, and engaged the consultancy KPMG to undertake an independent review of the incident.

In this case, the compliance notice provided a template for the Bank to report on to us. It outlined improvements the Bank needed to make to ensure the safety and security of the personal information in its care, building on the KMPG report.

CASE STUDY

Improving privacy practice in the rental sector

We prioritised rental sector privacy practices in 2021 due to growing concern over a power imbalance between tenants and landlords due to a shortage in the housing market.

We saw that some property management agencies were asking for very detailed information from prospective tenants as part of their selection process, while others were using public forums to compile lists of so-called 'bad tenants'.

Recognising that tenants had little power to challenge those responsible for their housing security, we took a proactive stance to protect the rights and privacy of tenants and prospective tenants.

We started by working with key stakeholders from both sides to understand the sector and the issues within. Based off this information, we developed new guidance for tenants, landlords, and others in the rental accommodation sector to clarify what information may be requested at every stage of the rental process, as well as a reporting tool for tenants to confidentially email us about their rental experiences.

We developed our communications and compliance approaches, including a compliance monitoring programme that involved regular checks of rental sector agencies and an annual survey of key documents, such as application forms and privacy policies.

We undertook initial monitoring and review on the impact the guidance had on the rental sector and the way organisations were operating within it. There are promising early signs that this has resulted in a significant reduction in the amount of personal information being collected from people who are looking for a rental home – a good outcome for privacy.

This work will continue in 2022/2023 as we continue to monitor uptake and compliance with the guidelines.



Objective 4 | Whāinga 4

We influence privacy practices and behaviour

Ka whakaawe mātou i ngā mahi me ngā whanonga matatapu

We work to ensure we are positively influencing organisations to develop their own workplace cultures founded on respecting personal information. Our ability to influence has been essential over the past year to ensuring privacy is a central consideration for government when it creates and implements policy and law.

We exert our influence in a range of ways: the people we partner with, how we communicate, the issues we choose to raise, the impact seen from our influence, and the data we produce to support our positions.

Over the past year, we have continued to be active in seeking to ensure that privacy is a central consideration when policy and law is being developed. As well as the extensive work we have done to support the public health response to COVID-19, we have provided input into a wide range of law reform or major policy processes.

Supporting Aotearoa New Zealand's COVID-19 response

We devoted significant resource to responding to national COVID-19-related issues, whether arising from the Government, organisations, or members of the public. Highlights included:

- Input into the roll-out of COVID-19 response measures to the Ministry of Health – Manatū Hauora, Department of the Prime Minister and Cabinet, and other agencies. This included workplace vaccination rules, and initiatives to manage COVID-19 at the border.
- Intervening in High Court judicial review proceedings concerning the Ministry of Health – Manatū Hauora and its responses to the Whānau Ora Commissioning Agency requests for Māori vaccination data. We provided expert submissions on the operation of the “serious threat to public health” exception in the Health Information Privacy Code and the Privacy Act.

- We consolidated and expanded our online information relating to COVID-19 and privacy.
- In late 2021, we managed a large peak in public enquiries about the Government's privacy considerations of COVID-19 and vaccination certificates, in particular the inclusion of people's date of birth on their vaccination certificate.

Influencing legislation development

As the Government's policy changes in response to COVID-19 decreased in early 2022, we have shifted focus to those elements of the Government's policy programme that have significant privacy elements. Highlights included:

- The proposed Income Insurance Scheme, which requires personal information to operate. We emphasised the importance of undertaking and publishing privacy analysis in support of the Scheme.
- Engaging with the Ministry of Business, Innovation and Employment (MBIE) investigation into the impacts of the December 2021 changes to the Credit Contracts and Consumer Finance Act 2003 and regulations. We encouraged the Ministry to consider amendments to the regulations minimising the amount of personal information lenders collect while still achieving the consumer protection objectives.

- Providing feedback to MBIE on the proposed regulatory regime for the Consumer Data Right.
- Providing advice on the Government's Fair Pay Agreements Bill.
- Our submission to the Governance and Administration Committee on the Data and Statistics Bill. This submission confirmed our broad comfort with the adequacy of safeguards in the Bill to protect individual privacy having engaged with Stats NZ during the policy development process, while also proposing additional safeguards for the Committee's consideration.

CASE STUDY

Intervening in judicial review

In 2021, the Whānau Ora Commissioning Agency (WOCA) requested Māori vaccination data in the North Island, to approach Māori about COVID-19 vaccination. The Ministry of Health – Manatū Hauora declined to share the level of detail requested, so WOCA twice took the issue to the High Court for judicial review.

At the heart of these proceedings were government decisions about the use of Māori data in responding to the pandemic and mitigating the serious public health risk and specific risk to Māori. This raised important questions about the role of tikanga Māori in the Ministry's decision-making process with tikanga evidence before the Court.

We intervened to share expert insight into how the Privacy Act can be used as a "how to" not a "do not do".

We provided submissions on the operation of the "serious threat to public health" exception in the Health Information Privacy Code and the Privacy Act under pandemic conditions.

The "serious threat to public health" exception is highly relevant in the Government's pandemic decision-making and an important component of the privacy framework.

The Court agreed with the Commissioner's submissions that urgent decision-making within a tight timeframe cannot be a "counsel of perfection" before information is disclosed in response to an evident threat to public health.

The Court required the Ministry to reconsider its response to the requests for vaccination data based on an evidence-based assessment.

The Ministry released the requested information shortly after the second judgment. It did so under certain conditions such as the requirement for WOCA to securely delete the information by the end of June 2022.

CASE STUDY

Privacy Week 2022: Privacy – The Foundation of Trust

Privacy Week usually centres around a forum or conference event, primarily attended by people who already care about privacy or work in the space. The focus was on teaching and telling, with talks and presentations for attendees.

In the spirit of trust, this year we tried a new approach to Privacy Week. We collaborated with Aotearoa New Zealand's privacy community to put on a week of virtual events and activities, only some of which we hosted ourselves. This flexible format meant more space for different types of events on topics related to privacy and trust.

As we broadened our engagement work to connect with new audiences, this was an opportunity for us to also use Privacy Week as a forum for listening and learning. Privacy Week 2022 was an experiment in partnership, collaboration, and new types of events to help us understand our audiences and how to best support them.

After reaching out to partners, friends, and the privacy community, we crafted a programme of 15 virtual and two in-person events, all of which were free. We ran some sessions, others were run in partnership, and some were entirely run by others.

We received more than 2,700 registrations across all events, with a 60% attendance rate of registrants following through. Fourteen members of our wider team spoke and presented at various events.

We chose to focus the week itself on increasing connections with new-to-privacy and new-to-OPC audiences, and this was successfully achieved, with over half of participants being first-time attendees to one of our events.

OPC-led sessions included:

- Safeguarding Children's Data Privacy in a Digital World
- Privacy 101 for DHB staff
- Tikanga Māori and Privacy: Reflections from the High Court Review of Decisions about Māori COVID-19 Vaccination Data
- Privacy for Schools
- Where Privacy Meets Power: Questions of Data and Racial Inequality
- Customer Privacy: The Journey from Compliance to Customer Trust

Partner events were:

- Privacy in 2022: What Does Good Look Like
- Inside, Outside, Upside Down: Intergovernmental Organisations and Data Protection
- The First 72 Hours after a Cyber Attack
- Cyber Incident Response Best Practice
- Navigating Privacy Changes in Property Management
- Learning from COVID-19: Building a Privacy Toolbox for Future Emergencies
- Measuring Trust

Office and functions | Te Tari me āna mahi



Independence and competing interests | Te noho motuhake me te taupatupatu o ngā hiahia

The Privacy Commissioner has wide ranging functions. The Commissioner must have regard to the information privacy principles in the Privacy Act and the protection of important human rights and social interests that compete with privacy.

Competing social interests include the desirability of a free flow of information and the right of government and business 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 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 matching programmes.

Reporting | Te tuku pūrongo

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 | Kaimahi

We employ staff in our Auckland and Wellington offices. The senior leadership team is made up as follows:

The Assistant Commissioner, Policy and Operations/Chief Operating Officer is responsible for 3 teams – Investigations and Dispute Resolution, Policy, and Compliance and Enforcement.

In November 2021 the Assistant Commissioner, Policy and Operations/Chief Operating Officer was appointed Deputy Privacy Commissioner for a twelve-month term. The Deputy Privacy Commissioner retained the same responsibilities held in her previous role.

The Assistant Commissioner, Strategy and Insights is responsible for the Strategy and Insights team and Communications and Engagement team.

The General Manager is responsible for administrative and managerial services. We employ administrative support staff in both offices.

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

COVID-19 | KOWHEORI-19

The Covid-19 pandemic has continued to affect the Office and functions of the Privacy Commissioner during the year to 30 June 2022.

The IT architecture of the Office was shaped by the lessons of the Kaikōura earthquake and the consequent need to be able to work remotely for extended periods. The Office continues to maintain business continuity of systems through cloud-based servers on the Microsoft Azure platform in Sydney. We use Microsoft Office 365 for office productivity and an Enterprise Content Management System for the secure storage and access, including secure remote access, of our information records.

The Office has a flexible working policy and remote working is further supported by video conferencing via Zoom to facilitate interaction across all staff, and with outside parties when required.

Statutory remuneration disclosures | Whakapuakitanga ā-Ture i ngā Taiutu

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.

Total remuneration and benefits	Number of employees	
	Actual 2022	Actual 2021
\$100,000 – \$109,999	3	5
\$110,000 – \$119,999	1	2
\$120,000 – \$129,999	1	
\$130,000 – \$139,999	1	
\$140,000 – \$149,999	1	1
\$150,000 – \$159,999	2	2
\$160,000 – \$169,999	1	
\$170,000 – \$179,999		1
\$180,000 – \$189,999	2	
\$240,000 – \$249,999	2	
\$320,000 – \$329,999	1	
\$330,000 – \$339,999		1

Commissioners' total remuneration

In accordance with the disclosure requirements of section 152(1)(a) of the CEA, the total remuneration includes all benefits paid during the period 1 July 2021 to 30 June 2022.

Name	Position	Amount 2022	Amount 2021
John Edwards	Privacy Commissioner (to 31 December 2021)	241,546	335,568
Liz MacPherson	Deputy Privacy Commissioner*/ Acting Privacy Commissioner from 10 December 2021	211,769	–

*Deputy Privacy Commissioner role commenced on 24th November 2021.

Cessation payment

During the 2022 year, there were no payments made in relation to cessation (2021: \$18,333).

Indemnity and Insurance disclosures

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

EEO profile | Pūkete EEO

The Office of the Privacy Commissioner promotes Equal Employment Opportunities (EEO) to ensure our people capability practices are in line with our obligations as a good employer.

We have an EEO policy integrated into the human resource programmes that are outlined in our Statement of Intent 2020-2024. The policy encourages active staff participation in all EEO matters. We review the policy regularly, together with policies on recruitment, employee development, harassment prevention, and health and safety.

During the year, the main areas of focus continue to be:

- developing talent regardless of gender, ethnicity, age, or other demographic factors
- integrating work practices which promote or enhance work life balance amongst employees, including family-friendly practices, flexible working, and health and wellbeing initiatives
- maintaining equitable gender-neutral remuneration policies which are tested against best industry practice
- placing a strong emphasis on fostering a diverse workplace and an inclusive culture.



We do not collect information on employees' age or disabilities. Where a disability is brought to our attention, we take steps to ensure that the employee has the necessary support to undertake their duties.

Our recruitment policies, including advertisement, comply with the good employer expectations of Diversity Works New Zealand, of which we are a member.

We have formal policies regarding bullying, harassment, and the provision of a safe and healthy workplace. Staff have ready access to external support through our employee assistance programme.

Workplace gender profile

as at 30 June 2022

Role	 Women		 Men		Total
	Full-time	Part-time	Full-time	Part-time	
Acting Privacy Commissioner	1				1
Senior managers	2		1		3
Team and unit managers	2	2	2		6
Investigations and Dispute Resolution	6	3	2		11
Administrative support	3	2	2		7
Policy	4		1	1	6
Compliance and Enforcement	2	1	1		4
Strategy and Communications	1		2	1	4
Legal	1	1			2
Total	22	9	11	2	44

Finance and performance report | Pūrongo whakahaere pūtea me ngā tutukitanga



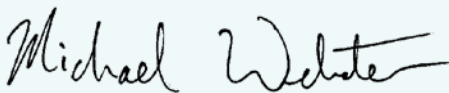
Statement of responsibility | Tauākī noho haepapa

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 2022.



M Webster
Privacy Commissioner
31 March 2023



G F Bulog
General Manager
31 March 2023

Completion of Audit

The Office of the Privacy Commissioner was required under section 156(1)(a) of the Crown Entities Act to complete its audited financial statements and statement of performance by 31 December 2022. This timeframe was not met due to the late completion of the audit.

Statement of performance | Tauākī tutukitanga





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 2020-2024 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 addition to the high-level objectives, the Office also identified three strategic priorities for the 2021/22 year. A summary of the key work undertaken within each of these is also highlighted in the introduction section and noted above.

The Statement of Performance Expectations for the year to June 2022 identified five output areas (primary activities) to support these objectives and priorities. These are consistent with the previous year and we report our progress against these Primary Activities in this section with linkage through to the objectives, where appropriate, using the following symbols:

-  **Objective 1** – Privacy protection is effective and easy to achieve
-  **Objective 2** – Costs of privacy compliance are minimised
-  **Objective 3** – OPC is trusted as a fair and responsive regulator
-  **Objective 4** – OPC influences privacy practices and behaviours

Impact of the COVID-19 emergency on performance | Te pāpātanga o te urutā KOWHEORI-19 ki ngā tutukitanga

Whilst the risk and uncertainties associated with COVID-19 have reduced overall during the year to 30 June 2022, the Auckland Office, in particular, was impacted with the restrictions during August- December 2021. Staff were however able to work from home and service delivery continued across the Office.

Reliable data and information remained available in order to report against all measures, and performance against most measures has been achieved. This is consistent with the prior year.

Due to the unpredictable nature of Covid-19, we are not able to determine the longer-term impacts of the pandemic on either our financial or non-financial performance with confidence. We will, however, continue to regularly monitor this risk.

PBE FRS 48 service performance reporting | PBE FRS 48 Pūrongo Tutukitanga Ratonga

PBE FRS48 replaces the service performance reporting requirements of PBE IPSAS 1 Presentation of Financial Statements and is effective for the year ending 30 June 2023, with earlier adoption permitted. The Privacy Commissioner has determined that the main impact of the new standard is that additional information will need to be disclosed on those judgements that have the most significant effect on the selection, measurement, aggregation and presentation of service performance information.

Statement specifying comprehensive income | Tāuāki tautohu whiwhinga whānui

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

Specified comprehensive income	Target \$000	Achievement \$000
Operating grant	7,392	7,392
Other revenue	194	405
Total revenue	7,586	7,797

The appropriation received by the Privacy Commissioner equals the government's actual expenses incurred in relation to the appropriations, which is a required disclosure from 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 2.5% of the total Vote Justice Non-Departmental Output Expenses Appropriation for 2021/22. The total expenses in the year are \$6,932,000 as set out in the cost of service statement below.

Cost of service statement | Tauākī utu ratonga

for the year ended 30 June 2022 |
mō te tau i eke i te 30 o Pipiri 2022

As set out in the 2021/22 Statement of Performance Expectations, the Privacy Commissioner committed to provide five primary activities. The split of funds across these five primary activities is set out below:

	Actual 2022 \$000	Budget 2022 \$000	Actual 2021 \$000
PRIMARY ACTIVITY 1: COMMUNICATION AND EDUCATION			
Resources employed			
Revenue	1,020	1,102	768
Expenditure	994	1,143	871
Net Surplus/(Deficit)	26	(41)	(103)
PRIMARY ACTIVITY 2: ADVICE AND ADVOCACY			
Resources employed			
Revenue	1,561	1,487	1,196
Expenditure	1,334	1,443	1,112
Net Surplus/(Deficit)	227	44	84
PRIMARY ACTIVITY 3: COMPLIANCE AND ENFORCEMENT			
Resources employed			
Revenue	1,801	1,705	1,975
Expenditure	1,549	1,658	1,732
Net Surplus/(Deficit)	252	47	243
PRIMARY ACTIVITY 4: INVESTIGATION AND DISPUTE RESOLUTION			
Resources employed			
Revenue	1,957	1,825	1,727
Expenditure	1,694	1,781	1,491
Net Surplus/(Deficit)	263	44	236

	Actual 2022 \$000	Budget 2022 \$000	Actual 2021 \$000
PRIMARY ACTIVITY 5: STRATEGY AND INSIGHTS			
Resources employed			
Revenue	1,458	1,467	1,869
Expenditure	1,361	1,502	1,844
Net Surplus/(Deficit)	97	(35)	25
TOTALS			
Resources Employed			
Revenue	7,797	7,586	7,535
Expenditure	6,932	7,527	7,050
Net Surplus/(Deficit)	865	59	485

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 which is consistent with prior years:

Criteria	Rating
On target or better	Achieved
<5% away from target	Substantially achieved
>5% away from target	Not achieved



Primary activity 1 | Mahi matua 1

Strategy and insights | Rautaki me ngā

Activity areas of focus

Understanding trends and technological developments that will be relevant in the future. Using evidence based on all inputs, including complaints, media, breach reporting, enquiries, international regulators or website analytics, to prioritise work and make decisions. Monitor success of strategies and initiatives. Advising the Commissioner on the best way to achieve the Office's mission as well as associated risks.

Output Measures

Measure	Estimate	Achieved 2021/22	Achieved 2020/21
Number of cross office priorities focussed on globally identified privacy trends or systematic issues. 	4	4 During the year, the Office was focussed on the following priority areas – Rental Sector, Biometrics, Embedding Te Ao Māori perspectives and the IPCA joint inquiry.	Not applicable – new measure for 2021/22
Number of published “insights” reports on trends that the Office is seeing. ¹ 	3	Not achieved – 2 In December 2021, the Office published an Insights Report on Privacy Breach Reporting and a further report was published in May 2022 covering awareness, knowledge and levels of concern regarding privacy amongst the general public.	Not applicable – new measure for 2021/22

¹ This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation and was the same as the SPE target.

Primary activity 2 | Mahi matua 2





Communications and education |

Whakapāpātanga, mātauranga hoki

Activity areas of focus

Informing people about their privacy rights. Promoting privacy understanding and competence, using media, opinion writing, events and conferences, stakeholder engagement. Producing material and resources to inform, guide and educate. Reduce the need for enforcement and dispute resolution through education.

Output Measures

Measure	Estimate	Achieved 2021/22	Achieved 2020/21
Education module completions as a percentage of education module registrations in the year. 	75%	Achieved – 79%	Not applicable – new measure for 2021/22.
Percentage uptake on media comments made by the Office. 	95%	Not achieved – 48% Of the 184 media enquiries received in the year to 30 June, the Office provided substantive comment on 181. Of this 181, 87 were then included in reporting.	Achieved – 95% 293 media enquiries were received and 95% of these were responded to with a substantive comment or information provided by the Office. ²
Percentage of media enquiries that are responded to within 2 working days. 	100%	Achieved – 100% All of the 184 media enquiries were responded to within 2 working days.	Not applicable – new measure for 2021/22.
Respond to all enquiries within 2 working days. ³ 	95%	Substantially achieved – 94%	Substantially achieved – 90%

2 The initial intention of the KPI was to report on how much uptake there was, following a comment being made. This was not possible to report in 2020/21 and so the Office reported on overall response rates to enquiries. The 2021/22 result shows the actual uptake following a response. By way of comparison, the actual response rate in 2021/22 was 98%.

3 This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation and was the same as the SPE target.




Primary activity 3 | Mahi matua 3

Compliance and enforcement | Te tautukunga me te whakauruhi

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, enforcement of policy work to ensure compliance.

Output Measures

Measure	Estimate	Achieved 2021/22	Achieved 2020/21
<p>The percentage of data breach notifications received through NotifyUs that are triaged within 1 working day.⁴</p> 	95%	Achieved – 95%	Not applicable – new measure for 2021/22.
<p>The percentage of externally reviewed compliance notices and Access Directions issued that meet quality review standards.⁵</p> 	100%	Not measured. An external review was not undertaken this year due to the low number of notices and access directions issued.	Not applicable – new measure for 2021/22.
<p>The percentage of information matching files reviewed within the mandatory 5-year period as required under S184 of the Privacy Act.</p> 	100%	Achieved All reviews are up to date although no information matching provisions were due a 5-year review in the 12 months to 30 June 2022.	Not applicable – new measure for 2021/22.

⁴ This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation and was the same as the SPE target.

⁵ As per footnote 4 above.

Primary activity 4 | Mahi matua 4




Advice and advocacy |

Te tohutohu me te taunaki

Activity areas of focus

Research and analysis supports advice on privacy issues that is context aware, evidence based and clear and informed. Advice reflects diverse perspectives and recognises risks and competing interests. Effective interventions include the development of privacy codes and advice to government on changes to other legislation. Advocate for privacy positive outcomes, including privacy by design.

Output Measures

Measure	Estimate	Achieved 2021/22	Achieved 2020/21
<p>The percentage of externally reviewed policy and information sharing are rated as 3.5 out of 5 or better for quality.⁶</p> 	85%	Achieved – 95%	Achieved – 85% ⁷
<p>The Commissioner actively contributes on advice, guidelines and directions by international institutions and guiding bodies, relating to the advancement of privacy rights.</p>  	Achieved	<p>Achieved</p> <p>The Office of the Privacy Commissioner has continued to support the development of international advice, guidelines, and directions, over the past year.</p> <p>We have been closely engaged in supporting the Ministry of Justice and Ministry of Foreign Affairs in discussions with the European Union on New Zealand's adequacy status. We have also attended multiple iterations of the Asia Pacific Privacy Authorities (APPA) forum, as well as the Global Privacy Assembly in October 2021, where we engaged in a range of discussions on pressing privacy matters and supported resolutions.</p>	Not applicable – new measure for 2021/22.

⁶ This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation and was the same as the SPE target.

⁷ The prior year result was against a slightly different measure that also included Information Matching files.




Primary activity 5 | Mahi matua 5

Investigations and dispute resolution | Ngā whakatewhatewha, whakatau tautohe hoki

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 and issuing compliance notices and access directions.

Output Measures

Measure	Estimate	Achieved 2021/22	Achieved 2020/21
<p>The percentage of notified complaints files closed by settlement between the parties.⁸</p> 	40%	<p>Achieved – 63%</p> <p>The Office has continued to focus on reaching settlement in the year.</p>	Achieved – 65% ⁹
<p>The percentage of externally reviewed complaints investigations that are rated as 3.5 out of 5 or better for quality.¹⁰</p> 	90%	<p>Achieved – 100%</p>	Achieved – 97.5%
<p>The percentage of complaint files closed during the year that were less than 6 months old at closure.¹¹</p> 	85%	<p>Not achieved – 67%</p> <p>The Office has had fewer, more complex complaints to deal with. Due to the nature of these complaints, the time taken to resolve them has been longer but the rate of settlement (as seen above) has remained high.</p>	Not applicable – new measure for 2021/22.

8 This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation and was the same as the SPE target.

9 The wording of the prior year measure was slightly different and related to all complaints closed and not just those that had been notified.

10 As per footnote 8.

11 As per footnote 8.

Statement of accounting policies | Tauākī kaupapa-here kaute

for the year ended 30 June 2022 |
mō te tau i eke i te 30 o Pipiri 2022

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 2022 and were approved by the Commissioner on 31 March 2023. 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 \$30m 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 2022:

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

Statement of comprehensive revenue and expenses | Tauākī whiwhinga, whakapaunga whānui

for the year ended 30 June 2022 |
mō te tau i eke i te 30 o Pipiri 2022

	Note	Actual 2022 \$000	Budget 2022 \$000	Actual 2021 \$000
Revenue				
Crown revenue	2	7,392	7,392	7,276
Other revenue	2	405	194	259
Total income		7,797	7,586	7,535
Expenditure				
Promotion	4	97	184	580
Audit fees		34	34	33
Depreciation and amortisation	4,8,9	294	310	235
Rental expense	4	427	431	450
Operating expenses	4	974	1,139	1,230
Contract services	4	90	203	373
Staff expenses	3	5,016	5,226	4,149
Total expenditure		6,932	7,527	7,050
Surplus/(Deficit)		865	59	485
Other comprehensive revenue and expenses		-	-	-
Total comprehensive revenue and expenses		865	59	485

Explanations of major variances are provided in Note 1.

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

Statement of changes in equity | Tauākī rerekētanga o te whai tūtanga

for the year ended 30 June 2022 |
mō te tau i eke i te 30 o Pipiri 2022

	Note	Actual 2022 \$000	Budget 2022 \$000	Actual 2021 \$000
Total equity at the start of the year		1,581	1,489	1,096
Total comprehensive revenue and expenses for the year		865	59	485
Total equity at the end of the year	5	2,446	1,548	1,581

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 | Tauākī Tūnga Pūtea

as at 30 June 2022 |
mō te tau i eke i te 30 o Pipiri 2022

	Note	Actual 2022 \$000	Budget 2022 \$000	Actual 2021 \$000
Public equity				
General funds	5	2,446	1,548	1,581
Total public equity		2,446	1,548	1,581
Current assets				
Cash and cash equivalents	6	2,008	1,057	1,272
Receivables	7	57	35	80
Prepayments	7	158	100	115
Total current assets		2,223	1,192	1,467
Non-current assets				
Property, plant and equipment	8	380	197	293
Intangible assets	9	255	596	333
Capital work in progress	8,9	–	–	115
Total non-current assets		635	793	741
Total assets		2,858	1,985	2,208
Current liabilities				
Payables	10	147	160	205
Employee entitlements	12	249	260	400
Total current liabilities		396	420	605
Non-current liabilities				
Lease incentive	11	16	17	22
Total non-current liabilities		16	17	22
Total liabilities		412	437	627
Net assets		2,446	1,548	1,581

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

Statement of cash flows | Tauākī kaupapa-here kaute

for the year ended 30 June 2022 |
mō te tau i eke i te 30 o Pipiri 2022

	Actual 2022 \$000	Budget 2022 \$000	Actual 2021 \$000
CASH FLOWS FROM OPERATING ACTIVITIES			
Cash was provided from:			
Receipts from the Crown	7,392	7,392	7,276
Receipts from other revenue	395	192	394
Interest received	6	2	1
Cash was applied to:			
Payment to suppliers	1,685	1,987	2,743
Payments to employees	5,166	5,230	4,067
Net Goods and Services Tax	(27)	(42)	30
Net cash flows from operating activities	969	411	831
CASH FLOWS FROM INVESTING ACTIVITIES			
Cash was applied to:			
Purchase of property, plant and equipment and intangibles	233	330	652
Cash was provided from:			
Sale of property, plant, and equipment and intangibles	–	–	–
Net cash flows from investing activities	(233)	(330)	(652)
Net increase/(decrease) in cash held	736	81	179
Plus opening cash	1,272	976	1,093
Closing cash balance	2,008	1,057	1,272
Cash and bank	2,008	1,057	1,272

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 | He pitopito kōrero mō ngā tauākī kaute

for the year ended 30 June 2022 |
mō te tau i eke i te 30 o Pipiri 2022

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 surplus is higher than the budgeted surplus by \$806k. This is primarily due to the following:

Staff expenses (down on budget by \$210k)

A number of staff departures and related vacancies have resulted in the salary costs being lower than budgeted.

Promotion costs (down on budget by \$87k)

The costs associated with the annual Privacy Awareness Week/Forum and Education services were less than predicted. In particular, rather than holding an in-person forum, as in previous years, a week of virtual events and activities – a "Privacy Festival" – was held instead which resulted in lower event related expenses.

Other operating expenses (down on budget by \$165k)

The two main areas that were under budget for the year were Travel (under budget by \$115k) and Litigation (under budget by \$74k). Travel costs were lower due to the travel restrictions due to COVID-19.

Contract Services (down on budget by \$113k)

The Office did not require the use of contractors in some of the areas that had been expected. In some areas, staff recruitments were used instead to fulfil the budgeted work – for example the triaging of complaints.

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 (2021: \$nil).

Other revenue breakdown

	Actual 2022 \$000	Actual 2021 \$000
Other grants received	316	161
Forums and conferences	-	19
Other revenue	83	78
Interest revenue	6	1
Total other revenue	405	259

Note 3: Staff expenses

Accounting policy

Superannuation schemes

Defined contribution schemes

Obligations for contributors to Kiwi Saver and the National Provident 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 2022 \$000	Actual 2021 \$000
Salaries and wages	4,982	3,917
Employer contributions to defined contribution plans	136	114
Other staff expenses	49	36
Increase/(decrease) in employee entitlements	(151)	82
Total staff expenses	5,016	4,149

Note 4: Other expenses

Accounting policy

Operating leases

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

Grant expenditure

Discretionary grants are those grants where the Office of the Privacy Commissioner has no obligation to award the grant on receipt of the grant application. Discretionary grants with substantive conditions are expensed when the grant conditions have been satisfied.

Critical judgements in applying accounting policies

Grant expenditure

During the 2020 financial year, the Privacy Commissioner approved 4 discretionary grants under its Privacy Good Research Fund with the aim of stimulating privacy related research by external entities. The conditions include milestones and specific requirements. The Office of the Privacy Commissioner has accounted for the related grant expenses when evidence of meeting these milestones has been received from the recipient. Not all the research was completed within the 2020 and 2021 year. A final total of \$5k was expensed in relation to these grants in 2022 (2021: \$11k). All milestones have now been met in relation to these approved grants.

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 2022 \$000	Actual 2021 \$000
Fees paid to auditors:		
External audit – current year	34	33
Promotion costs:		
Website expenses	55	109
Privacy Week / Forum	16	17
Other marketing expenses	26	454
Total promotion expenses	97	580
Depreciation and amortisation:		
Furniture and fittings	43	59
Computer equipment	51	39
Office equipment	13	9
Intangibles	187	128
Total depreciation and amortisation	294	235
Rental expense on operating leases	427	450
Contract services	90	373
Other operating expenses:		
Computer maintenance/licences	321	320
Staff travel	22	48
Staff development	87	48
Loss on disposal	2	31
Grant expenditure	5	11
Recruitment	58	192
Utilities	253	251
Other	199	329
Total other operating expenses	974	1,230

Operating leases as lessee

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

	Actual 2022 \$000	Actual 2021 \$000
Not later than one year	417	426
Later than one year and not later than five years	1,312	1,589
Later than five years	–	141
Total non-cancellable operating leases	1,729	2,156

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 will expire in December 2025.

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

During 2019, the Privacy Commissioner entered a new agreement for the lease of Zoom Room equipment. The term is for 36 months and will end in October 2022.

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 2022 \$000	Actual 2021 \$000
Opening balance	1,581	1,096
Net (deficit)/surplus	865	485
Closing balance	2,446	1,581

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 2022 \$000	Actual 2021 \$000
Cash on hand and at bank	56	54
Cash equivalents – on call account	1,952	1,218
Total cash and cash equivalents	2,008	1,272

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 face value, less an allowance for expected losses.

	Actual 2022 \$000	Actual 2021 \$000
Receivables	57	80
Prepayments	158	115
Total	215	195
Total receivables comprise:		
GST receivable (exchange transaction)	53	80
Other receivables (non-exchange)	4	-
Total	57	80

The carrying value of receivables approximates their fair value.

The carrying amount of receivables that would otherwise be past due, but not impaired, whose terms have been renegotiated is \$nil (2021: \$nil).

Note 8: Property, plant and equipment

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.

Revaluations

The Privacy Commissioner has not performed any revaluations of property, plant or equipment.

Depreciation

Depreciation is provided on a straight-line basis on all property, plant and equipment, at a rate which will write off the cost (or valuation) 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.

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.

Breakdown of property, plant and equipment and further information

	Furniture and fittings \$000	Computer equipment \$000	Office equipment \$000	Total \$000
Cost				
Balance at 1 July 2020	515	187	77	779
Additions	182	44	1	227
Disposals	(489)	(10)	(3)	(502)
Balance at 30 June 2021	208	221	75	504
Balance at 1 July 2021	208	221	75	504
Additions	69	86	29	184
Disposals	–	(41)	(16)	(57)
Transfers from Work in Progress	11	–	–	11
Balance at 30 June 2022	288	266	88	642
Accumulated depreciation and impairment losses				
Balance at 1 July 2020	420	111	44	575
Depreciation expense	59	39	9	107
Elimination on disposal	(459)	(9)	(3)	(471)
Balance at 30 June 2021	20	141	50	211
Balance at 1 July 2021	20	141	50	211
Depreciation expense	43	51	13	107
Elimination on disposal	–	(40)	(16)	(56)
Balance at 30 June 2022	63	152	47	262
Carrying amounts				
At 30 June 2021	188	80	25	293
At 30 June 2022	225	114	41	380

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 2022 (2021: \$72k).

Work in progress

The capital work in progress figure is \$nil as at 30 June 2022 (2021: \$11k).

Note 9: Intangible assets

Accounting policy

Software acquisition

Acquired computer software licences are capitalised based on the costs incurred to acquire and bring to use the specific software.

Staff training costs are recognised as an expense when incurred.

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	50%–25%
Interactive tools	3 years	33.3%

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.

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 5 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
- 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

In April 2021, the IASB's Interpretation Committee issued an agenda decision that clarified the accounting treatment expected for customisation and configuration costs associated with software as a service (SAAS) arrangements. In the 2021 Annual Report, the Privacy Commissioner identified \$222,894 of assets that were believed to be related to SAAS arrangements that had been previously capitalised. There was insufficient time to fully consider the impact of the agenda decision in time for the 2021 year-end.

A detailed review of the assets making up the \$222,894 was undertaken for the year ended 30 June 2022. As a result, most of the assets were determined to not be SAAS related and therefore no adjustment was required. Two remaining assets with a total cost of \$87k were deemed to be SAAS related. Of these, one has now been fully written down as at 30 June 2022 and the net book value of the remaining asset is only \$9k.

Due to the immateriality of the balances identified, no historical accounting adjustments have been made in the accounts for the year ended 30 June 2022.

Movements for each class of intangible asset are as follows:

	Acquired software \$000	Interactive tools \$000	Total \$000
Cost			
Balance at 1 July 2020	145	258	403
Additions	14	255	269
Disposals	–	–	–
Transfers from Work in Progress	–	83	83
Balance at 30 June 2021 / 1 July 2021	159	596	755
Additions	–	7	7
Disposals	–	(54)	(54)
Transfers from Work in Progress	–	103	103
Balance at 30 June 2022	159	652	811
Accumulated amortisation and impairment losses			
Balance at 1 July 2020	70	224	294
Amortisation expense	44	84	128
Disposals	–	–	–
Balance at 30 June 2021 / 1 July 2021	114	308	422
Amortisation expense	29	158	187
Disposals	–	(53)	(53)
Balance at 30 June 2022	143	413	556
Carrying amounts			
At 30 June and 1 July 2021	45	288	333
At 30 June 2022	16	239	255

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 2022 (2021: \$10k).

Work in progress

The Capital Work in Progress figure for 2022 is \$nil (2021: \$103k).

Note 10: Payables

Accounting policy

Creditors and other payables are recorded at the amount payable.

Breakdown of payables

	Actual 2022 \$000	Actual 2021 \$000
Payables under exchange transactions		
Creditors	87	149
Accrued expenses	53	50
Lease incentive	7	7
Total payables under exchange transactions	147	205
Payables under non-exchange transactions		
Other payables	-	-
Total payables under non-exchange transactions	-	-
Total creditors and other payables	147	205

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 2022 \$000	Actual 2021 \$000
Lease incentive	16	22
Total non-current liabilities	16	22

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.

The Privacy Commissioner recognises a liability and an expense for bonuses where it is contractually obliged to pay them, or where there is a past practice that has created a constructive obligation. No such liability is included as at 30 June 2022 (2021: \$nil).

Breakdown of employee entitlements

	Actual 2022 \$000	Actual 2021 \$000
Current employee entitlements are represented by:		
Accrued salaries and wages	–	139
Annual leave	249	261
Total current portion	249	400
Current	249	400
Non-current	–	–
Total employee entitlements	249	400

Note 13: Contingencies

There are no known contingencies existing at balance date (2021: \$nil). The Privacy Commissioner used to be subject to “Make Good” clauses in its lease contracts but there are no such clauses included in the current contracts.

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.

Key management personnel compensation

	Actual 2022 \$000	Actual 2021 \$000
Total salaries and other short-term employee benefits	1,178	981
Full-time equivalent members	4.4	4.6

Key management personnel include all Senior Managers and the Privacy Commissioner who together comprise the Senior Leadership Team (SLT). The Privacy Commissioner left at the end of December 2021 and the Deputy Privacy Commissioner appointed in November 2021 became the Acting Privacy Commissioner for the remainder of the financial year.

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:

	2022 \$000	2021 \$000
FINANCIAL ASSETS		
Financial assets measured at amortised cost		
Cash and cash equivalents	2,008	1,272
Receivables (excluding prepayments and taxes receivables)	4	–
Total loans and receivables	2,012	1,272
FINANCIAL LIABILITIES		
Financial liabilities at amortised cost		
Payables (excluding income in advance, taxes payable, grants received subject to conditions and lease incentive)	140	199
Total financial liabilities at amortised cost	140	199

Note 17: COVID-19 financial impact assessment

Impact of COVID-19

During August to December 2021 the Auckland region moved to Alert Levels 4 and 3. During this time, the Auckland office remained closed.

The Wellington region moved to Alert Level 4 and 3 during August 2021 and finally to Level 2 on 7 September 2021. Due to the end of the COVID-19 Alert system on 2nd December 2021, and the move to the Covid Protection Framework, there have been no further lock-downs affecting the Office.

Impact on operations

The Privacy Commissioner has offices in both Wellington and Auckland, so this meant staff were required to work from home at Alert Level 4 and 3. The impact that this had on the ability for the Office to deliver on its key services was limited. As noted previously, the Office had already updated its IT infrastructure and this aided in the ability for staff to work remotely.

Revenue

There was no impact on Crown revenue.

Expenditure

Some areas of expenditure are lower than budgeted due to COVID-19. Most notably, the travel related costs. In addition, the accumulated leave balance has continued to remain high as staff holiday plans have been impacted. This is being actively monitored by the Senior Leadership Team.

The Office provided a small Data and Communications allowance to staff when they were required to work from home due to the COVID-19 lock downs. This totalled \$7k for the year to 30 June 2022.

Other significant assumptions

There are no provisions made for COVID-19 impact within the Privacy Commissioner's balance sheet and no further significant assumptions have been made concerning the future impact. The Office is not aware of any other uncertainties at the reporting date that pose a significant risk of causing material adjustment to the carrying balances of assets and liabilities within the next financial year.

Appendices | Ngā Tāpiritanga



Appendix A | Tāpiritanga A

Processes and services |

Ngā Tukanga me ngā Ratonga

Dispute resolution

Our Investigations and Dispute Resolution Team investigates complaints from the public about interferences with individuals' privacy. They work with parties to achieve a fair outcome using various dispute resolution techniques.

An interference with privacy occurs when an agency has breached a privacy principle and caused the complainant harm, such as physical or emotional harm, or financial loss (however, a complainant does not have to demonstrate harm where the complaint is about access to or correction of information).

During an investigation we determine whether the respondent agency has breached the Privacy Act and if the complainant has suffered harm that requires a remedy, such as an apology or compensation. We can compel agencies to produce documents and meet with complainants. We cannot compel complainants or respondents to accept settlement terms and we cannot award damages. However, our view is an important indication of whether there's been an interference with privacy.

We try to reach a settlement of the complaint at every point in the process.

If we have not been able to resolve a complaint, usually the complainant can take their case to the Human Rights Review Tribunal.

In some exceptional circumstances, we may refer a case to the Director of Human Rights Proceedings. The Director can then choose whether to bring the case before the Human Rights Review Tribunal.

In some cases, the team will decline to investigate where an investigation would be unnecessary or inappropriate. They'll always try to provide people with reasons they cannot investigate, and if they can, refer them to another agency that might be able to help them.

Advice and advocacy

We provide advice to a range of organisations on the privacy risks of various initiatives. We also offer advice to help organisations mitigate privacy risks.

Our advice is sometimes solicited from agencies that are looking to amend internal policy, and we sometimes proactively provide advice on upcoming legislation. This is generally in the form of submissions to Select Committees, but we also provide input into Cabinet Papers and may brief Cabinet Committees in person.

We also engage with the private sector to consult on a variety of projects, such as Privacy Impact Assessments. This is a growing area as more private sector organisations manage their privacy risk by engaging with our team early in technology deployment projects.

Information sharing and matching

A significant portion of our work involves Approved Information Sharing Agreements (AISAs). These are agreements between government agencies that allow them to share information with one another. We consult on these agreements and highlight potential risks.

Information matching involves the comparison of one set of records with another, generally to find records in both sets that belong to the same person.

Information matching raises several privacy issues, such as the potential to disclose incorrect date information or the potential to 'automate away' human judgement.

One of the Commissioner's functions is to require government departments to report on their operation of authorised information matching programmes and, in turn, report to Parliament with an outline of each programme and an assessment of each programme's compliance with the Privacy Act.

Communications and engagement

Our Communications and Engagement Team works to raise privacy awareness and engage with stakeholders. We work through many channels, producing material such as:

- speeches and presentations for the Commissioner
- media releases and advisories
- blog posts
- social media content
- case notes
- our monthly newsletter.

We also produce guidance to help make privacy easy. A key part of this is our e-learning modules. We have worked with education experts to build a suite of online courses covering various aspects of privacy and continue to develop new courses to meet changing needs.

We respond to enquiries from journalists and the public via traditional media as well as social media.

Compliance and enforcement

This team is responsible for identifying and assessing systemic issues and using the right tools to get the best privacy outcomes for New Zealanders. The team's work includes enforcing the Codes, managing privacy breach responses, prosecution, issuing of compliance notices where necessary, and monitoring of compliance, enforcement, or policy work to ensure compliance.

Strategy and insights

This team is responsible for understanding trends and developments, both nationally and internationally, that will be relevant in the future. Insights Reports are produced to share this trend intelligence. Using evidence from all the Office's activities, the team helps to prioritise delivery of work and services accordingly. Following prioritisation, the team will monitor the success of the strategies and initiatives put into place and will advise the Commissioner on the best way for the Office to achieve on its mission. This team also leads the Office's work to engage and partner with Māori.

Appendix B | Tāpiritanga B

Information Matching 2021/22 |

Te Whakataurite Pārongo 2021/22

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.

This year I issued one report reviewing information matching provisions.

Births, Deaths, Marriages, and Relationships Registration Act 1995, section 78A; Citizenship Act 1977 (s 26A), Corrections Act 2004 (s 181), and Immigration Act 2009 (s 294), Customs and Excise Act 2018 (s 310). Immigration Act 2009 (s 295), Tax Administration Act 1994 (Schedule 7 Part C subpart 2 cl 43)

This report covered six provisions:

- Births, Deaths, Marriages, and Relationships Registration Act 1995, section 78A – which provides for death information to be provided to Immigration New Zealand to enable updating of overstayer and temporary visa holder records.
- Citizenship Act 1977, s 26A enabling the Department of Internal Affairs to provide citizenship information to Immigration New Zealand, to remove new citizens from the overstayer records.
- Corrections Act 2004, s 181 and Immigration Act 2009, s 294 enabling the Department of Corrections to provide information to Immigration New Zealand, to identify prisoners who fall within the deportation provisions of the Immigration Act as a result of their criminal convictions.
- Customs and Excise Act 2018, s 310 to improve the enforcement of fines by identifying serious fines defaulters as they cross New Zealand borders.

- The Immigration Act 2009, s 295 enabling Immigration New Zealand to provide contact information of people crossing the border to the Ministry of Justice, to locate people who have outstanding fines in order to enforce payment.
- Tax Administration Act 1994, Schedule 7 Part C subpart 2 cl 43 enabling the Inland Revenue Department to provide contact details to the Ministry of Justice, to locate people who have outstanding fines in order to enforce payment.

I considered that the authority conferred by these information matching provisions should be continued without amendment. However, I intend to review the utility of s 295 of the Immigration Act 2009 again in 12 months as it is currently not used.

Review report are available on our website: <https://privacy.org.nz/privacy-for-agencies/information-sharing/information-matching-reports-and-reviews/>

Changes in information matching programmes

Current programmes

There were 46 information matching programmes in operation, and 10 programmes that were not active.

Of the active programmes nine were not compliant. The issues were all either already known to the Ministry of Social Development, or were identified by them during reviews.

- An enquiry form used for the social welfare reciprocity arrangement with Australia is not deleted when no longer required;
- Birth and death, and name change information, used in two programmes, is not deleted from the matching system after a successful match;
- A letter explaining information matching is not sent for six social welfare reciprocity programmes (those with Canada, Denmark, Greece, Ireland, Guernsey and Jersey, and the United Kingdom). This Notice of Information Matching is intended to be sent when the superannuation arrangement is set-up for each client to explain that letters about changes will be sent when changes are made, rather than being sent before any record is adjusted.

A warning has been given in relation to this non-compliance.

These are all either under investigation, or remedies are in development. I will monitor this progress and take formal enforcement action if necessary.

New provisions and programmes

Parliament passed no new information matching provisions during the year. No new programmes commenced operation during the year.

Programmes ceasing

As advised in 2020, four of the current information matches between different functions of the Department of Internal Affairs are being replaced by new processes conducted under an Approved Information Sharing Agreement. The "Information Sharing Agreement between the Department of Internal Affairs and the Registrar-General, Births, Deaths and Marriages" was authorised by an Order-in-Council on 17th December 2018 (Privacy (Information Sharing Agreement between Department of Internal Affairs and Registrar-General) Order 2018 (2018/275)). DIA are still in the process of modifying their work processes and systems. When these changes are complete they will operate the information sharing under the AISA.





- Births, Deaths, Marriages, and Relationships Registration Act 1995, s 78A: -
 - BDM/DIA Passports
 - BDM Births & Marriages/ Citizenship applications
- Citizenship Act 1977, s 26A: -
 - Citizenship/DIA Passports
 - Citizenship/BDM Citizenship by Birth




Other information matches involving birth, death, marriage and name change information from DIA to various agencies are also intended to be transferred to AISAs.









How we assess programme compliance








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.

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.
-  **Inactive** – where the programme has not been operated during the year.

<p>Accident Compensation Act 2001, s 246 and Tax Administration Act 1994, Schedule 7 Part C subpart 2 cl 41</p>	<p>Compliance</p>
<p>1. IR/ACC Compensation and Levies To confirm income amounts for compensation calculations. 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>	
<p>Accident Compensation Act 2001, s 280</p>	<p>Compliance</p>
<p>2. Corrections/ACC Prisoners To ensure that prisoners do not continue to receive earnings-related accident compensation payments. 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>	
<p>Accident Compensation Act 2001, s 281</p>	<p>Compliance</p>
<p>3. 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. ACC disclosure to MSD: ACC selects individuals who have either:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>	

Births, Deaths, Marriages, and Relationships Registration Act 1995, s 78A	Compliance
<p>4. BDM (Births)/IR Newborns Tax Number</p> <p>To enable birth information to be confirmed in order to allocate an IR number to a new-born child.</p> <p>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.</p>	
<p>5. BDM (Births)/MoE Student Birth Confirmation</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>BDM disclosure to Ministry of Education: BDM provides names, gender, date of birth of New Zealand-born citizens.</p>	
<p>6. BDM (Births)/MoH NHI and Mortality Register</p> <p>To verify and update information on the National Health Index and to compile mortality statistics.</p> <p>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.</p>	
<p>7. BDM/MSD Identity Verification</p> <p>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.</p> <p>BDM disclosure to MSD: BDM provides birth and death information for the 90 years prior to the extraction date.</p> <p>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.</p> <p>Not compliant – minor technical issue – information retained.</p>	
<p>8. BDM (Deaths)/GSF Eligibility</p> <p>To identify members or beneficiaries of the Government Superannuation Fund (GSF) who have died.</p> <p>BDM disclosure to GSF: BDM provides information from the NZ Deaths Register covering the 12 weeks prior to the extraction date. The information includes full name at birth, full name at death, gender, date of birth, date of death, place of birth, and number of years lived in New Zealand (if not born in New Zealand).</p>	
<p>9. BDM (Deaths)/INZ Deceased Temporary Visa Holders</p> <p>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.</p> <p>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.</p>	
<p>10. BDM (Deaths)/IR Deceased Taxpayers</p> <p>To identify taxpayers who have died so that IR can close accounts where activity has ceased.</p> <p>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.</p>	
<p>11. BDM (Deaths)/MoH NHI and Mortality Register</p> <p>To verify and update information on the NHI and to compile mortality statistics.</p> <p>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.</p>	

Births, Deaths, Marriages, and Relationships Registration Act 1995, s 78A (continued)	Compliance
<p>12. BDM (Deaths)/MSD Deceased Persons</p> <p>To identify current clients who have died so that MSD can stop making payments in a timely manner.</p> <p>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.</p>	
<p>13. BDM (Deaths)/NPF Eligibility</p> <p>To identify members or beneficiaries of the National Provident Fund (NPF) who have died.</p> <p>BDM disclosure to NPF: BDM provides information from the NZ Deaths Register covering the 12 weeks prior to the extraction date. The information includes full name at birth, full name at death, gender, date of birth, date of death, place of birth, and number of years lived in New Zealand (if not born in New Zealand).</p>	
<p>14. BDM (Deaths)/NZTA Deceased Driver Licence Holders</p> <p>To improve the quality and integrity of data held on the Driver Licence Register by identifying licence holders who have died.</p> <p>BDM disclosure to Waka Kotahi 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.</p>	
<p>15. BDM (Marriages)/MSD Married Persons Benefit Eligibility</p> <p>To identify current clients who have married so that MSD can update client records and reassess their eligibility for benefits and allowances.</p> <p>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.</p>	
<p>16. BDM/DIA (Citizenship) Citizenship Application Processing</p> <p>To verify a parent's citizenship status if required for determining an applicant's eligibility for New Zealand citizenship.</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>	
<p>17. BDM/DIA(Passports) Passport Eligibility</p> <p>To verify, by comparing details with the Births, Deaths and Marriages registers, whether a person is eligible for a passport, and to detect fraudulent applications.</p> <p>BDM disclosure to Passports (DIA): Possible matches from the Births, Deaths and Marriages (relationships) databases are displayed to Passports staff as they process each application. The details displayed include full name, gender and date of birth.</p>	
<p>18. BDM/MSD Overseas Born Name Change</p> <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>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> <p>Not compliant – minor technical issue – information retained.</p>	

Citizenship Act 1977, s 26A	Compliance
<p>19. DIA (Citizenship)/BDM Citizenship by Birth Processing</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>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>	
<p>20. DIA(Citizenship)/DIA(Passports) Passport Eligibility</p> <p>To verify a person's eligibility to hold a New Zealand passport from Citizenship database information.</p> <p>Citizenship (DIA) disclosure to Passports (DIA): Possible matches from the Citizenship database are displayed to Passports staff as they process each application. The possible matches may involve one or more records. The details displayed include full name, date of birth, country of birth and the date that citizenship was granted.</p>	
<p>21. DIA(Citizenship)/INZ Entitlement to Reside</p> <p>To remove from the Immigration New Zealand (INZ) overstayer records the names of people who have been granted New Zealand citizenship.</p> <p>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.</p>	
Corrections Act 2004, s 180	Compliance
<p>22. Corrections/MSD Prisoners</p> <p>To detect people who are receiving income support payments while imprisoned, and to assist MSD in the recovery of outstanding debts.</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>	
Corrections Act 2004, s 181 and Immigration Act 2009, s 294	Compliance
<p>23. Corrections/INZ Prisoners</p> <p>To identify prisoners who fall within the deportation provisions of the Immigration Act 2009 as a result of their criminal convictions, or are subject to deportation because their visa to be in New Zealand has expired.</p> <p>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.</p> <p>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.</p>	

Customs and Excise Act 2018, s 306**Compliance****24. 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.

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).

**25. Customs/IR Student Loan Interest**

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.

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.

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.

**Customs and Excise Act 2018, s 307****Compliance****26. Customs/IR Child Support Alerts**

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.

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.

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).

**Customs and Excise Act 2018, s 309****Compliance****27. Customs/MSD Periods of Residence**

To enable MSD to confirm periods of residence in New Zealand or overseas to determine which other countries, with superannuation reciprocity agreements with New Zealand, an individual may be eligible to claim superannuation payments from.

Customs disclosure to MSD: Customs provides MSD access to its CusMod system for verification of departure and arrival dates.





**Customs and Excise Act 2018, s 310****Compliance****28. 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.

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.



Education and Training Act 2020, schedule 3 cl 9	Compliance
<p>29. MoE/Teaching Council Registration</p> <p>To ensure teachers are correctly registered (Teaching Council) and paid correctly (Ministry of Education).</p> <p>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.</p> <p>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).</p>	
Education and Training Act 2020, schedule 9 cl 7	Compliance
<p>30. MoE/MSD (Study Link) Results of Study</p> <p>To determine eligibility for student loans and/or allowance by verifying students' study results.</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>	
Education and Training Act 2020, schedule 9 cl 8 & 9	Compliance
<p>31. Educational Institutions/MSD (Study Link) Loans and Allowances</p> <p>To verify student enrolment information to confirm entitlement to allowances and loans.</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>	
Electoral Act 1993, s 263A	Compliance
<p>32. INZ/EC Unqualified Voters</p> <p>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.</p> <p>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.</p>	

33. DIA (Citizenship)/EC Unenrolled Voters

To compare the Citizenship database with the electoral roll so that people who are qualified to vote but have not enrolled may be invited to enrol.

Citizenship (DIA) disclosure to Electoral Commission: Citizenship provides full name, date of birth and residential address of new citizens aged 17 years and over (by grant or by descent).

**34. DIA (Passports)/EC Unenrolled Voters**

To compare passport records with the electoral roll to:

- identify people who are qualified to vote but have not enrolled so that they may be invited to enrol
- update the addresses of people whose names are already on the roll.

Passports (DIA) disclosure to Electoral Commission: Passports provides full name, date of birth and residential address of passport holders aged 17 years and over.

**35. MSD/EC Unenrolled Voters**

To compare MSD's beneficiary and student databases with the electoral roll to:

- identify beneficiaries and students who are qualified to vote but who have not enrolled so that they may be invited to enrol
- update the addresses of people whose names are already on the roll.

MSD disclosure to Electoral Commission: MSD provides full name, date of birth and address of all individuals aged 17 years or older for whom new records have been created or where key data (surname, given name or address) has changed, provided these records have not been marked as confidential.

**36. NZTA (Driver Licence)/EC Unenrolled Voters**

To compare the Driver Licence Register with the electoral roll to:

- identify people who are qualified to vote but have not enrolled so that they may be invited to enrol
- update the addresses of people whose names are already on the roll.

NZTA disclosure to Electoral Commission: NZTA provides the full name, date of birth and address of driver licence holders aged 17 and over whose records have not been marked confidential.

**37. NZTA (Vehicle Registration)/EC Unenrolled Voters**





To compare the motor vehicle register with the electoral roll to:





- identify people who are qualified to vote but have not enrolled so that they may be invited to enrol
- update the addresses of people whose names are already on the roll.

NZTA disclosure to Electoral Commission: NZTA provides the full names, date of birth and addresses of individuals aged 17 and over who registered a vehicle or updated their details in the period covered by the extract. The 'Owner ID' reference number is also included to identify any multiple records for the same person.



Electronic Identity Verification Act 2012, s 39	Compliance
<p>38. DIA Identity Verification Service (IVS)</p> <p>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.</p> <p>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 stillborn indicator.</p> <p>Deaths disclosure to IVS: Names, gender, date of birth, place of birth, date of death, place of death and age at death.</p> <p>Marriages disclosure to IVS: Names, date of birth, date of marriage, registration number, country of birth, gender, place of marriage, spouse's names.</p> <p>Citizenship disclosure to IVS: Names, gender, date of birth, place of birth, photograph, citizenship person identifier, citizenship certificate number, certificate type and certificate status.</p> <p>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.</p> <p>Immigration disclosure to IVS: Whether a match is found, client ID number and any of the pre-defined set of identity related alerts.</p>	
Immigration Act 2009, s 295	Compliance
<p>39. INZ/Ministry of Justice Fines Defaulters Tracing</p> <p>To enable the Ministry of Justice to locate people who have outstanding fines in order to enforce payment.</p> <p>Justice disclosure to INZ: Justices sends INZ details of serious fine defaulters who have triggered a 'silent' alert as part of the linked Customs/Justice Fines Defaulters Alerts Programme. Each record includes the full name, date of birth, gender, passport number, Justice unique identifier number and flight information of the fines defaulter.</p> <p>INZ disclosure to Justice: INZ supplies information contained on the arrival and departure card, which includes full name, date of birth, gender, passport number, nationality, occupation, New Zealand address and date of expected return to New Zealand (in the case of a departing traveller).</p>	
Immigration Act 2009, s 300	Compliance
<p>40. INZ/MoH Publicly Funded Health Eligibility</p> <p>To enable the Ministry of Health to determine an individual's eligibility for access to publicly funded health and disability support services; or liability to pay for publicly funded health and disability support services received.</p> <p>MoH disclosure to INZ: MoH sends names, date of birth and NHI number to INZ for matching.</p> <p>INZ disclosure to MoH: INZ provides names, gender, birth date, nationality, visa or permit type and start and expiry dates, and dates the person entered or left New Zealand. INZ may also disclose details of a parent or guardian of a young person.</p>	
Motor Vehicle Sales Act 2003, s 120 and s 121	Compliance
<p>41. Customs/MBIE Motor Vehicle Traders Importers</p> <p>To identify people who have imported more than three motor vehicles in a 12 month period and are not registered as motor vehicle traders.</p> <p>Customs disclosure to MBIE: Customs provides MBIE with the full name, address, contact numbers and a Customs unique identifier of all individuals or entities that have imported more than three vehicles within the previous 12 months.</p>	

Motor Vehicle Sales Act 2003, s 122 and s 123	Compliance
<p>42. NZTA/MBIE Motor Vehicle Traders Sellers</p> <p>To identify people who have sold more than six motor vehicles in a 12-month period and are not registered as motor vehicle traders.</p> <p>NZTA disclosure to MBIE: NZTA provides MBIE with the full name, date of birth and address of all individuals or entities who have sold more than six vehicles in a 12-month period.</p> <p>MBIE disclosure to NZTA: MBIE provides NZTA with the full name, date of birth, address and trader unique identifier of new motor vehicle traders so that these traders are excluded from future match runs.</p>	
Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Australia) Order 2017	Compliance
<p>43. Australia (Centrelink)/MSD Change in Circumstances</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>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>Not compliant – minor technical issue – information retained.</p>	
Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Canada) Order 1996	Compliance
<p>44. Canada/MSD Social Welfare Reciprocity</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>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>Not compliant – 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>	
Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Denmark) Order 1997	Compliance
<p>45. Denmark/MSD Social Welfare Reciprocity</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>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>Not compliant – 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>	

Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Ireland) Order 1993	Compliance
<p>46. Ireland/MSD Social Welfare Reciprocity</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>Ireland disclosure to MSD: includes full name, date of birth, marital status, address, entitlement information and Social Security numbers.</p> <p>MSD disclosure to Ireland: includes full name, date of birth, marital status, address, entitlement information and MSD client number.</p> <p>Not compliant – 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>	
Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Jersey and Guernsey) Order 1995	Compliance
<p>47. Jersey and Guernsey/MSD Social Welfare Reciprocity</p> <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>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>Not compliant – 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>	
Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Malta) Order 2013	Compliance
<p>48. Malta/MSD Social Welfare Reciprocity</p> <p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and Malta.</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>	
Social Security Act 2018, s 380 and Social Welfare (Reciprocity with the Hellenic Republic) Order 1993	Compliance
<p>49. Hellenic Republic/MSD Social Welfare Reciprocity</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>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>Not compliant – 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>	

Social Security Act 2018, s 380 and Social Welfare (Reciprocity with the Netherlands) Order 2003 Compliance

50. Netherlands/MSD Change in Circumstances

To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and the Netherlands.

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.

Netherlands disclosure to MSD: SVB responds with the SVB reference number.



51. Netherlands/MSD General Adjustment

To enable the processing of general adjustments to benefit rates for individuals receiving pensions from both New Zealand and the Netherlands.

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.

Netherlands disclosure to MSD: SVB advises adjustments to payment rates and the 'holiday pay' bonus.



Social Security Act 2018, s.380 and Social Security (Reciprocity with the United Kingdom) Order 1990 Compliance

52. United Kingdom/MSD Social Welfare Reciprocity

To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and the United Kingdom.

UK disclosure to MSD: includes full name, date of birth, marital status, address, entitlement information and Social Security numbers.

MSD disclosure to UK: includes full name, date of birth, marital status, address, entitlement information and New Zealand Client Number.

Not compliant – Notice of Information Matching letter advising of process around changes to entitlement not sent, but adverse action letters advising of actual changes are sent.



Social Security Act 2018, Schedule 6, cl 13 Compliance




53. MSD/Justice Fines Defaulters Tracing

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

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 a data matching reference number to MSD.

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



<p>Social Security Act 2018, Schedule 6, cl 15</p>	<p>Compliance</p>
<p>54. Justice/MSD Warrants to Arrest</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>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>Tax Administration Act 1994, Schedule 7 Part C subpart 2 cl 43</p>	<p>Compliance</p>
<p>55. IR/Justice Fines Defaulters Tracing</p> <p>To enable the Ministry of Justice to locate people who have outstanding fines in order to enforce payment.</p> <p>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.</p> <p>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.</p>	
<p>Tax Administration Act 1994, Schedule 7 Part C subpart 2 cl 45</p>	<p>Compliance</p>
<p>56. IR/MSD (Netherlands) Tax Information</p> <p>To enable income information about New Zealand-resident clients of the Netherlands government insurance agencies to be passed to the Netherlands for income testing.</p> <p>IR disclosure to the Netherlands: For New Zealand-resident clients of the Netherlands government insurance agencies, IR provides the individual's contact details and income information to the Netherlands Sociale Verzekeringsbank (social insurance) or Uitvoeringsinstituut Werknemers Verzekeringen (employee insurance). MSD acts as liaison, forwarding requests to IR and forwarding the response to the Netherlands.</p>	

Appendix C | Tāpiritanga C Independent Auditor's Report | Pūrongo Kaitātāri Kaute Motuhake

To the readers of the Privacy Commissioner's financial statements and performance information for the year ended 30 June 2022

The Auditor-General is the auditor of the Privacy Commissioner. The Auditor-General has appointed me, Melissa Collier, using the staff and resources of Deloitte Auckland, to carry out the audit of the financial statements and the performance information, including the performance information for an appropriation, of the Privacy Commissioner on his behalf.

Opinion

We have audited:

- the financial statements of the Privacy Commissioner on pages 37 to 57, that comprise the statement of financial position as at 30 June 2022, 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 including a summary of significant accounting policies and other explanatory information; and
- the performance information of the Privacy Commissioner on pages 6 to 19 and 28 to 36.

In our opinion:

- the financial statements of the Privacy Commissioner on pages 37 to 57:
 - present fairly, in all material respects:
 - its financial position as at 30 June 2022; 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 the Public Benefit Entity Standards Reduced Disclosure Regime; and
- the performance information on pages 6 to 19 and 28 to 36:
 - presents fairly, in all material respects, the Privacy Commissioner's performance for the year ended 30 June 2022, including:
 - for each class of reportable outputs:
 - its standards of delivery performance achieved as compared with forecasts included in the statement of performance expectations for the financial year; and
 - its actual revenue and output expenses as compared with the forecasts included in the statement of performance expectations for the financial year; and
 - what has been achieved with the appropriations; and
 - the actual expenses or capital expenditure incurred compared with the appropriated or forecast expenses or capital expenditure.
 - complies with generally accepted accounting practice in New Zealand.

Our audit was completed on 31 March 2023. This is the date at which our opinion is expressed. We acknowledge that our audit was completed later than required by regulatory requirements. This was due to the auditor shortage in New Zealand.

The basis for our opinion is explained below. In addition, we outline the responsibilities of the Privacy Commissioner and our responsibilities relating to the financial statements and the performance information, we comment on other information, and we explain our independence.

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 and the International Standards on Auditing (New Zealand) 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 financial statements and the performance information

The Privacy Commissioner is responsible for preparing financial statements and performance information that are fairly presented and comply with generally accepted accounting practice in New Zealand. The Privacy Commissioner is responsible for such internal control as it is necessary to enable the Privacy Commissioner to prepare financial statements and performance information that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements and the performance information, the Privacy Commissioner is responsible for assessing the Privacy Commissioner's ability to continue as a going concern. The Privacy Commissioner is also responsible for disclosing, as applicable, matters related to going concern and using the going concern basis of accounting, unless there is an intention to merge or to terminate the activities of the Privacy Commissioner, or there is no realistic alternative but to do so.

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 financial statements and the performance information

Our objectives are to obtain reasonable assurance about whether the financial statements and the performance information, 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 these financial statements and the performance information.

For the budget information reported in the financial statements and the performance information, our procedures were limited to checking that the information agreed to the Privacy Commissioner's statement of performance expectations.

We did not evaluate the security and controls over the electronic publication of the financial statements and the performance information.

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 financial statements and the performance information, 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 the appropriateness of the reported performance information within the Privacy Commissioner's framework for reporting its performance.
- We conclude on the appropriateness of the use of the going concern basis of accounting by the Privacy Commissioner and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Privacy Commissioner's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our auditor's report to the related disclosures in the financial statements and the performance information or, if such disclosures are inadequate, to modify our opinion. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the Privacy Commissioner to cease to continue as a going concern.
- We evaluate the overall presentation, structure and content of the financial statements and the performance information, including the disclosures, and whether the financial statements and the performance information 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 responsible for the other information. The other information comprises the information included on pages 2 to 5, 20 to 27 and 58 to 75, but does not include the financial statements and the performance information, and our auditor's report thereon.

Our opinion on the financial statements and the performance information 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 financial statements and the performance information, our responsibility is to read the other information. In doing so, we consider whether the other information is materially inconsistent with the financial statements and the performance information 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 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.



Melissa Collier
Deloitte Auckland

On behalf of the Auditor-General
Auckland, New Zealand





Privacy Commissioner
Te Mana Mātāpono Matatapu

Published by the Office of the Privacy Commissioner
PO Box 10094
Wellington
109-111 Featherston Street
Wellington 6143
www.privacy.org.nz

© 2023 The Privacy Commissioner
ISSN 1179-9838 (Print)
ISSN 1179-9846 (Online)