

PRIVACY COMMISSIONER

Annual Report 2021



Annual Report of the Privacy Commissioner

for the year ended 30 June 2021

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 2021

A handwritten signature in blue ink, appearing to read 'John Edwards', is positioned above the printed name and title.

John Edwards
Privacy Commissioner
20 December 2021

Introduction	2
Privacy in Aotearoa New Zealand – the year in numbers	4
Key successes	6
Progress against strategic objectives	10
Nationwide media campaign: ‘Privacy is Precious’	21
Supporting the public health response to COVID-19	22
Shaping practice in the rental sector	23
Office and functions	24
Independence and functions	25
Reporting	25
Staff	26
COVID-19	26
EEO profile	27
Finance and performance report	28
Statement of responsibility	29
Statement of performance	30
Impact of the COVID-19 emergency on performance	31
Statement specifying comprehensive income	31
Cost of service statement for the year ended 30 June 2021	32
Primary activity 1: Strategy and Insights	34
Primary activity 2: Communications and education	36
Primary activity 3: Compliance and enforcement	38
Primary activity 4: Advice and advocacy	40
Primary activity 5: Investigations and dispute resolution	42
Statement of accounting policies	44
Statement of comprehensive revenue and expenses	46
Statement of changes in equity	47
Statement of financial position	48
Statement of cash flows	49
Notes to the financial statements	50
Appendices	62
Appendix A Processes and services	63
Appendix B Information matching 2020/21	65
Appendix C Independent Auditor’s Report	76

Introduction

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

This has been an extraordinary year. The Privacy Act 2020 came into effect, giving us a wider mandate and new compliance powers. We developed a new strategic framework and outcomes, and new tools to make privacy easy. We ran a major campaign to increase privacy awareness amongst everyday New Zealanders and to introduce agencies to their new obligations. And we did it all within a global pandemic, contributing ongoing guidance and advice to those working on Aotearoa New Zealand's COVID-19 response.

The protection and appropriate use of personal information has been critical to the success of the systems and tools developed by the Government and others to fight COVID-19. Good privacy practices have helped build trust as well as protect New Zealanders from COVID-19.

Good privacy outcomes are best achieved when everyone understands their rights and responsibilities and is motivated to act on them.

Since the new Act came into force in December 2020, we saw a 97% increase in the number of breaches reported to us in comparison to the preceding six months. More than half of those breaches involved emotional harm, and around one third resulted in a risk of identity theft or financial harm. Mandatory breach reporting will reveal to us over time the scale of serious privacy breaches in Aotearoa New Zealand.

It will also offer us lessons in how the breaches are happening and where our intervention will be most useful in addressing the biggest causes.

While our goal is to achieve high levels of voluntary compliance, we are taking a hard-line approach to regulatory action for wilfully non-compliant individuals or organisations.

The introduction of the Privacy Act 2020 and our subsequent budget increase allowed us to set up new ways of working, set our own agenda and identify ways to maximise our reach as a regulator.

We have been able to broaden our focus. Where previously we were obliged to identify individual harm, that's now just one of the factors that guides our interventions. We shifted towards being more proactive and thoughtful about how we meet the previously unmet needs of groups that are less vocal or visible.

We designed a Compliance and Regulatory Action Framework (CARAF) – a strategy document that sets out the principles which guide how we apply our new law, so that our decisions are better informed and there is a better understanding of emerging challenges.

Throughout the year, privacy issues emerged around the administration of COVID-19 vaccine delivery, testing, vaccination registers, and proof of immunisation. Our Office continues to work with the Ministry of Health to ensure that sensitive personal information is protected and disclosed only when necessary.



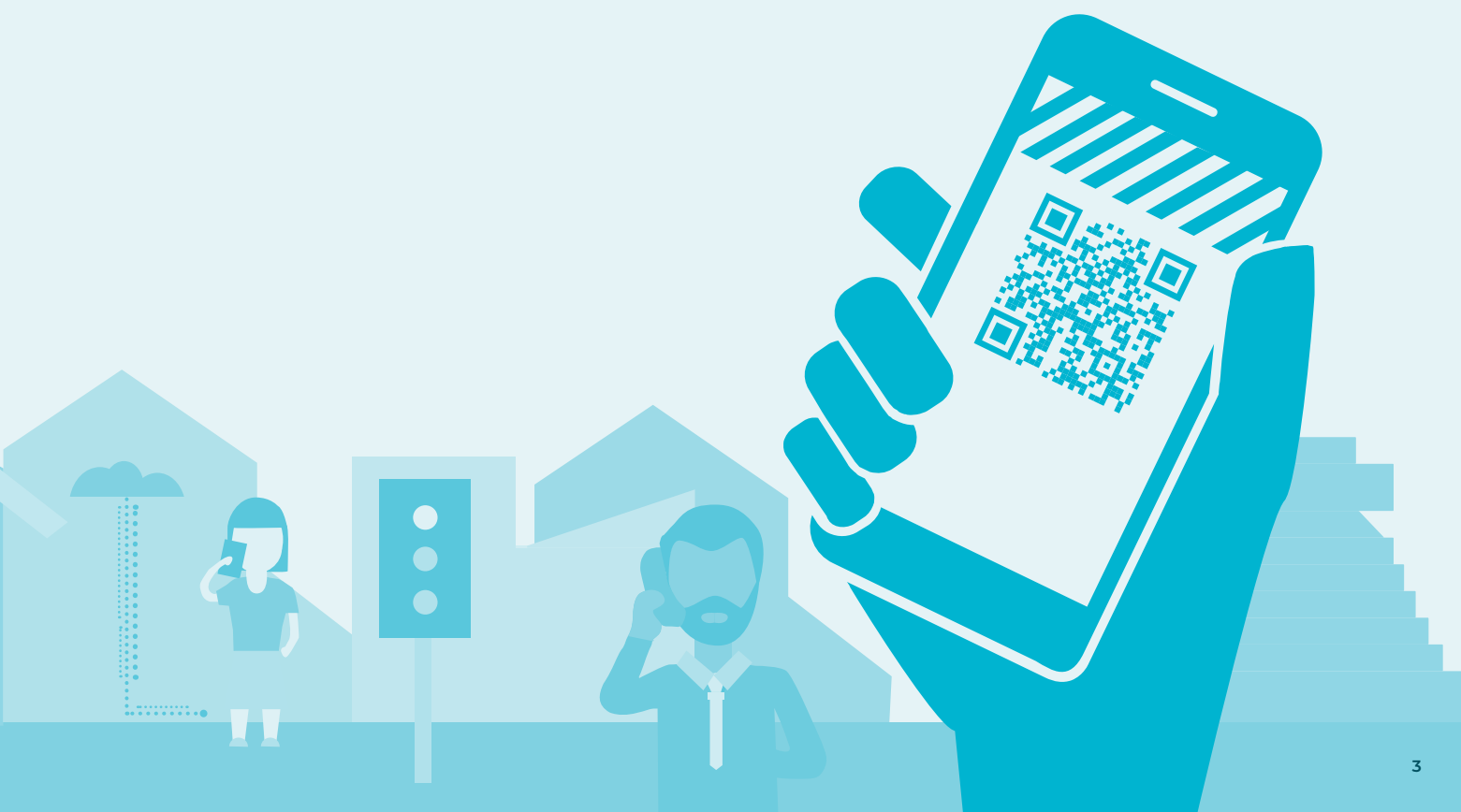
Following engagement with the rental accommodation sector on the collection, retention, and disclosure of personal information, we are providing clear guidance and will be increasingly using some of our enforcement tools against those who are purposefully not complying with the law.

We are committed to being more visible and relevant to Māori and have created the position of Principal Adviser Māori to help us achieve that goal.

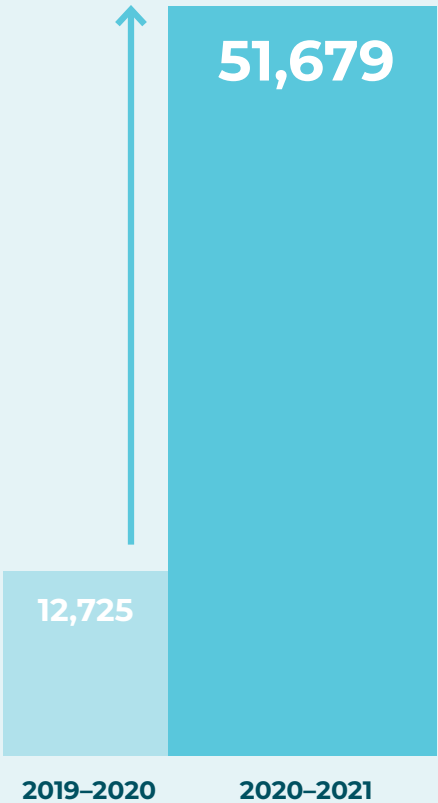
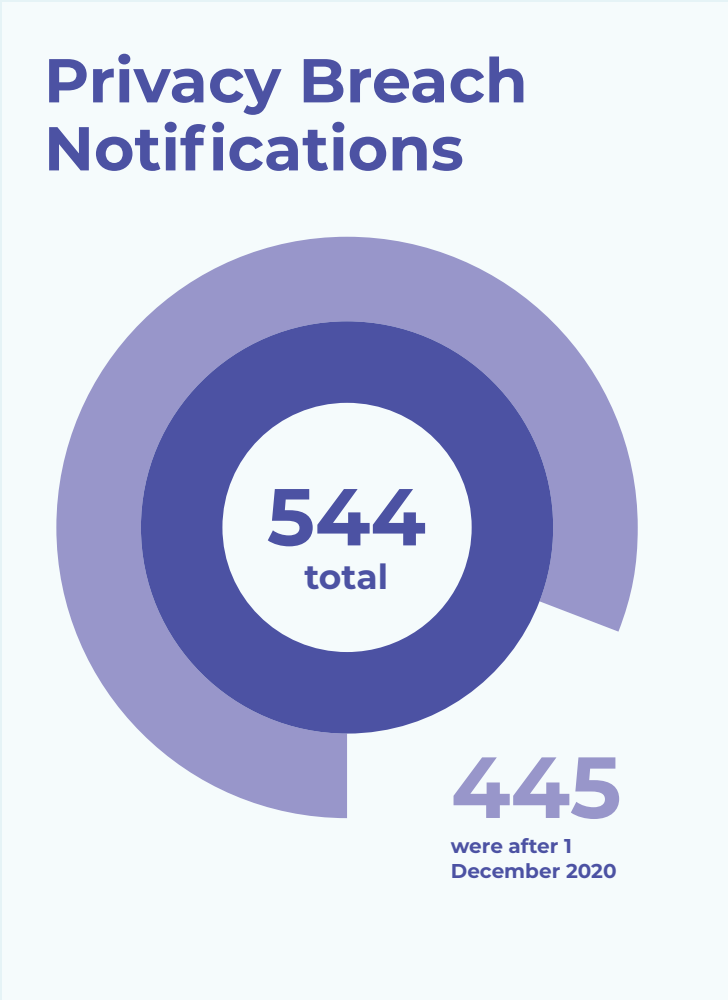
During my tenure as Privacy Commissioner, I have seen the institutions of the state, of commerce and industry, and of the non-government sector, come to embrace and internalise privacy values. We have come a long way from regarding privacy as a compliance issue, along with the myriad of regulatory requirements imposed on business and government, to seeing it as a precondition for the maintenance of trust and confidence. We have an informed and engaged public, and a strong and principled team at the Office of the Privacy Commissioner standing ready to safeguard privacy through the next set of challenges.

John Edwards
Privacy Commissioner

Good privacy outcomes are best achieved when everyone understands their rights and responsibilities and is motivated to act on them.



Privacy in Aotearoa New Zealand – the year in numbers



E-learning Modules Completed



561
Complaints Received



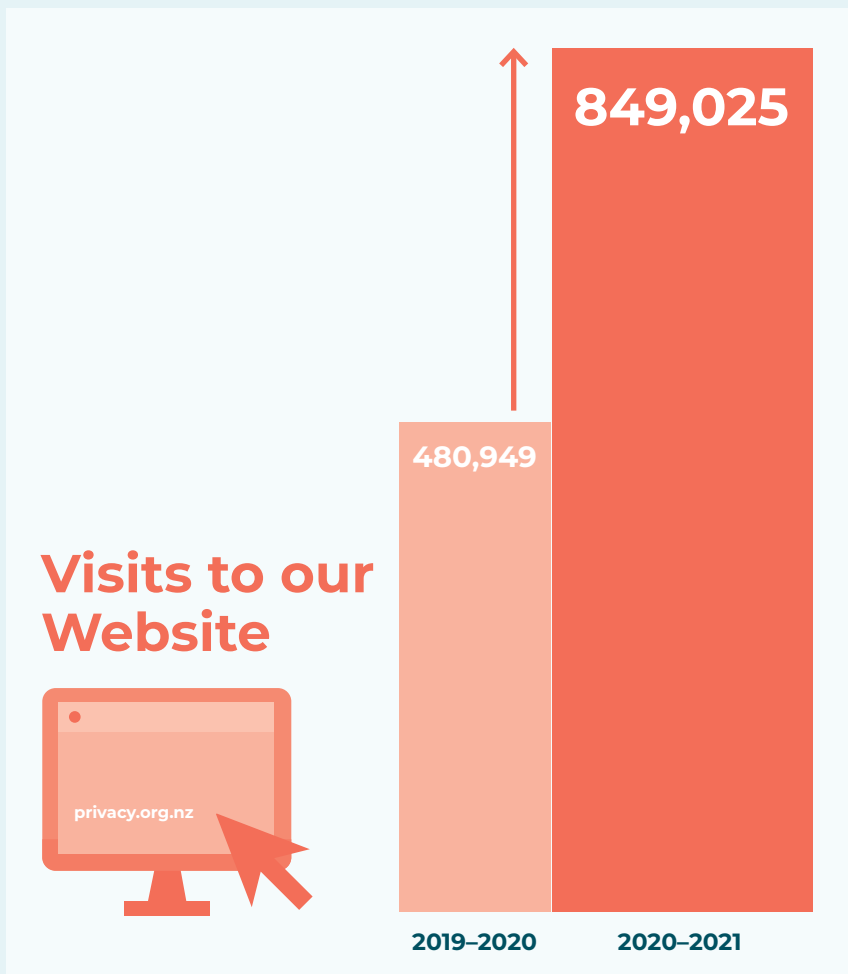
580
Complaints Closed



9,165
Enquiries Received



293
Media Enquiries Received



Key successes

Supporting the response to COVID-19

Supporting the public health response to COVID-19 has remained a key focus. Throughout the 2020-2021 year the Government developed a range of initiatives to manage Aotearoa New Zealand's response to the COVID-19 pandemic, many of which involve the use of personal information. They include the establishment of the Managed Isolation and Quarantine system, the development of contact tracing and record-keeping systems, and the early stages of the vaccination roll-out. We worked to ensure that sharing and use of personal information was enabled where it was needed to support the public health response, while ensuring that this was done in ways that were privacy protective. We were involved from the outset to ensure that privacy stayed clearly in frame during the development of the Covid tracer app.

As well as providing advice to Government on the public health response, we provided advice to agencies and individuals on Covid-related privacy issues as they emerged. Our advice on topics such as whether employers can tell their staff about a positive case in the workplace and privacy-protective record keeping for contact tracing purposes was read thousands of times. Through our enquiries service, we provided guidance directly to many New Zealanders who made enquiries about COVID-19 and their personal privacy.

Helping New Zealanders resolve their privacy problems

In a year of unprecedented disruption and change for our organisation, we have continued to help New Zealanders with their privacy problems. We closed 580 complaint files from individuals concerned about how their personal information had been treated and responded to 9,165 public enquiries from those with privacy-related questions.

Making international connections

The Office has contributed at global and regional networks such as the Global Privacy Assembly, Organisation for Economic Co-operation and Development (OECD), Asia-Pacific Economic Cooperation Data Subgroup (APEC DPS), and the Asia Pacific Privacy Authorities (APPA) Forum. This ensures that we are up to date with global privacy developments that could have an impact on Aotearoa New Zealand and can learn from our fellow regulators.

Through our enquiries service, we provided guidance directly to many New Zealanders who made enquiries about COVID-19 and their personal privacy.

Public interest investigations

In 2021-21, we initiated three inquiries.

On 12 August 2020 we released our report *Inquiry into Trade Me's Privacy Policy update and compliance with the Privacy Act 1993*. This Inquiry related to a change in how Trade Me allowed its members the ability to opt out of advertising. The Inquiry found that Trade Me did not take all reasonable steps to communicate how members' information could be used, causing confusion and a backlash among some members who had used the opt out.



On 11 September 2020 we released our report *Inquiry into illion's Arrangement with its related company Credit Simple*. illion is one of three credit reporters regulated under the Credit Reporting Privacy Code and the Inquiry found that illion breached the Code through their arrangement with their related company Credit Simple. The Inquiry found that illion circumvented the application of the Code for marketing purposes and the bundling of unrelated authorisations into a statutory right to access. As a result of the Inquiry illion and Credit Simple changed their operating practices in order to comply with the Code.

As well as supporting the ongoing COVID-19 public health response, we conducted an *Inquiry into the Ministry of Health's use and disclosure of patient information*. In April 2020 the Ministry of Health began disclosing COVID-19 patient information to emergency services to assist the response to the pandemic. In July the New Zealand Herald reported it had received the details of COVID-19 patients.

The results of a Public Service Commission Te Kawa Mataaho investigation into these disclosures were referred to us so that we could complete our own Inquiry into the situation. In September we found that while the Ministry of Health had a clear and measured rationale for its decisions to provide patient information to emergency services, these decisions should have been reviewed as the COVID-19 alert levels changed. We made several recommendations to improve how the Ministry of Health and Police used and disclosed COVID-19 patient information. This Inquiry was also an opportunity to make important findings into the application of the public health exception in the Privacy Act which applies where the collection, use, and disclosure of personal information is needed to combat a serious threat to public health.



A New Act

The Privacy Act 2020 came into force on 1 December 2020. It strengthens the principles-based approach to privacy to improve and protect the privacy of New Zealanders.

Important new changes include the following:

- A mandatory notifiable privacy breach regime was introduced so if agencies have a privacy breach that they believe has caused (or is likely to cause) serious harm, they must notify the Office of the Privacy Commissioner and consider notifying affected individuals.
- The Privacy Commissioner can issue compliance notices to direct agencies to start or stop doing something in order to comply with the Privacy Act.
- The Privacy Commissioner can direct agencies to provide individuals access to their personal information. This will allow faster resolution of complaints relating to information access under principle 6.
- A new privacy principle on disclosing personal information overseas was established. Under the new principle 12, an organisation or business may only disclose personal information to an agency outside Aotearoa New Zealand after assessing whether the information will be subject to similar safeguards to those in the Privacy Act.
- There are new criminal offences for misleading an organisation in order to access, use, alter, or destroy someone else's information, or destroying documents containing personal information if a request has been made for it. The penalty is a fine up to \$10,000.



1 December 2020

The Privacy Act 2020 came into force on 1 December 2020. It strengthens the principles-based approach to privacy to improve and protect the privacy of New Zealanders.



New ways of working

The new Act called for new tools and new approaches, as well as a new way of working.

To be an effective, modern privacy regulator we completed a review of our operating model, designed to create an organisation that is more strategic, more data driven, and more empowering of our staff. As a part of this we did an organisational restructure, with key changes including:

- a Strategy and Insights function to support us to take an intelligence-based approach to where we focus our effort
- a Principal Adviser Māori to support our work to be a good partner to Māori
- a Compliance and Enforcement team to take the lead on addressing systemic issues that may require the use of our enforcement tools.

To provide agencies with certainty about how we intend to approach our new enforcement role, we developed and published a Compliance and Regulatory Action Framework (CARAF) that sets out how we intend to use the full breadth of our powers to achieve the best privacy outcomes for all.

It is our belief that the most efficient and effective means of protecting individual privacy is for our Office to provide guidance and advice and for agencies to educate themselves. However, our stronger compliance powers will be used to hold agencies to account where necessary to address non-compliance.

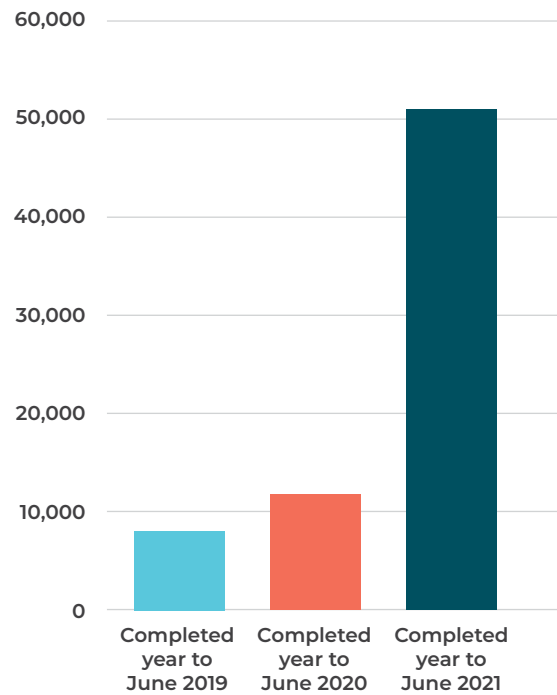
New tools to increase understanding

The new Privacy Act 2020 requires agencies and businesses to treat privacy differently, introducing mandatory reporting of serious breaches and giving the Privacy Commissioner compliance powers. Our Office developed and launched new tools, resources, and campaigns to raise awareness of the changes and assist agencies to comply with the new rules.

We released an online tool called NotifyUs in November 2020, just ahead of the legislative change. NotifyUs is an online self-assessment tool to guide agencies through the decision-making and reporting process for notifying privacy breaches. In this financial year, we received 544 breach notifications, 469 of these through the NotifyUs system.

We developed two new e-learning modules, *Privacy Act 2020* and *Privacy Breach Reporting* to help agencies, privacy officers and the public understand the implications of the law changes. We saw a 300% increase in e-learning completion this year, in large part due to the addition of these two new modules.

E-learning completions by year



To help increase awareness of the new Act, we ran our first nationwide public engagement campaign. Our 'Privacy is Precious' campaign ran in November and December 2020 and included television and digital advertising, as well as new information and resources.

We also re-issued our six Codes of Practice under the new Privacy Act on 1 December 2020:

- the Civil Defence National Emergencies (Information Sharing) Code 2020
- the Credit Reporting Privacy Code 2020
- the Health Information Privacy Code 2020
- the Justice Sector Unique Identifier Code 2020
- the Superannuation Schemes Unique Identifier Code 2020
- the Telecommunications Information Privacy Code 2020.

A new strategy

This year has been a pivotal one for the Office. Alongside the new Act, we set ourselves a new ambition to be an effective, modern privacy regulator – both in Aotearoa New Zealand and internationally. To accomplish this mission we set ourselves a new strategic framework:

Our strategy

Our mission

Who we are:

We are an effective modern privacy regulator, in New Zealand and internationally

Our primary activities

What we will do:



Focus of the SPE

Our objectives

How we create public and economic benefit and increase the wellbeing of New Zealanders:



Our priorities

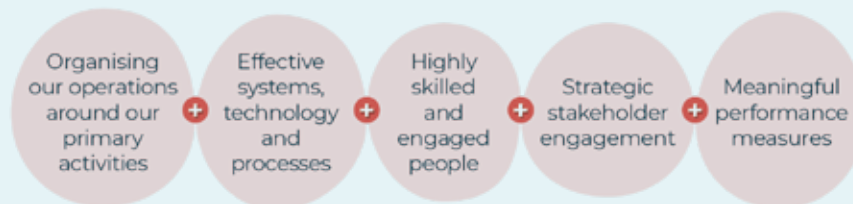
What we'll focus on:



Focus of the SOI

Our enablers

What we need to get there:



Our values

While upholding our values:



Progress against strategic objectives

Our Statement of Intent for the period June 2020 to June 2024 sets four key strategic objectives:



Objective 1: Privacy protection is effective and easy to achieve

When there is effective privacy protection and it is easy to achieve, individuals can engage in society knowing their privacy interests are being protected and promoted.

At the same time, organisations are empowered to use personal information in ways that respect privacy and that are commercially or socially beneficial. Making privacy easy makes it accessible and empowers people and organisations to lift their level of compliance and exercise their rights.

We continue to work to ensure that agencies have the tools and information available to them to easily meet their obligations under the Privacy Act. We provide advice and guidance on topical issues through our website, social media, newsletters, and enquiries service. In the lead up to the new Act's commencement, we developed new tools to help agencies meet their obligations and conducted an extensive, regional visits programme, giving presentations in Ōtautahi Christchurch, Te Papa-i-Oea Palmerston North, Tāmaki Makaurau Auckland, Ōtepoti Dunedin, Whakatū Nelson, Tauranga, Ngāmotu New Plymouth, Waihopai Invercargill, Te Mata-a-Māui Hawke's Bay, Tāhuna Queenstown, and Kirikiriroa Hamilton.

Law and lore working together to protect our most vulnerable

In 2016, Te Puea Memorial Marae in south Auckland opened its doors to homeless whānau across Tāmaki Makaurau Auckland. Five years later, the marae's Manaaki Tāngata e Rua transitional housing programme has helped over 500 people – of all ethnicities and backgrounds – into housing security. And they've done it with a strong focus on privacy and information protection.

Manaaki Tāngata e Rua facilitator Hurimoana Dennis worked closely with the OPC team to develop tools and knowledge that would enable them to provide wraparound support for whānau, including working across multiple government agencies. He says:

“Information sharing was a significant and critical feature of our Māori Service Delivery Model here at the Marae. The multitude of complicated issues that each whānau brought to the Marae as 'homeless' meant we have to act on and or advocate on their behalf.

“Information sharing is about sharing critical knowledge and information that will help whānau meet their needs, help the organisation meet their obligations, and ultimately build people's trust and confidence. It helps answer questions that have been difficult to get answers to and help them be understood and resonate.”

OPC attended a Hui alongside Manaaki Tāngata e Rua and Ministry of Social Development staff, speaking about how the privacy principles can operate to give agencies the freedom to continue doing good work in the community. This visit inspired Manaaki Tāngata e Rua to develop their own privacy policies and agreements and come up with tikanga-based approaches to best serve their community.

“The Tāmaki Makaurau Auckland OPC office reviewed our information-sharing systems and processes and followed through with training, a visit, and feedback. Now I think we know the Privacy Act and principles better than agencies and find ourselves educating them on what they can and can't do!”, says Hurimoana Dennis.



Hurimoana Dennis (centre) with members of the Manaaki Tāngata e Rua kaimahi, supplied by Hurimoana Dennis

“This support gave us confidence to do our mahi safely which we were able to pass on to our client whānau respectfully and confidently. Out of 502 homeless whānau, no one has refused to sign our information sharing protocols. They trust us, and we know how the law and the lore work together.”

Now, Ministry of Social Development staff and others work on the Marae alongside Manaaki Tāngata e Rua. By co-locating offices, and ensuring that information is being shared appropriately, safely, and with the mana of the individual of paramount consideration, they are making their services more accessible to some of Aotearoa New Zealand’s most vulnerable people.

No surprises advice on sharing personal information

There have been several instances over the years that highlight the complexity of Ministers’ use of information held by departments. We worked with the Crown Law Office to develop new guidance to assist government departments and Ministers when disclosing personal information.

Following consultation with Department of Prime Minister and Cabinet (DPMC) and the Public Service Commission (PSC), this guidance was released in December 2020 and was provided to Ministers and government departments as part of the briefing process for incoming Ministers after the 2020 election.

The role of Ministers is such that they can be provided with personal information to exercise statutory functions or respond to individuals seeking assistance with their cases. There are also times that the provision of personal information to a Minister may occur as the Minister is accountable to Parliament for their department’s actions and performance.

Our guidance reminds the public sector that the Privacy Act 2020 applies to both departments and Ministers, and that the disclosure of personal information from a department to a Minister must be lawful under the Privacy Act or an overriding statute. The Privacy Act regards a department and its Minister as separate agencies, and our guidance sets out the respective roles of each and how disclosures of personal information can be made.



Objective 2: Costs of privacy compliance are minimised

The decisions we make as we oversee compliance with the Privacy Act can have economic implications for individual agencies or for parts of the economy. The Act obliges us to take into account the case for government and business achieving their objectives in an efficient way.

As a modern regulator we will consider the consequences of different regulatory responses to an issue, including taking no action on a matter, balancing the public benefit against a range of factors, including the economic cost.

Our focus for this objective has been ensuring that we provide agencies with tools to make it easy for them to understand and comply with the new obligations that came into effect with the Privacy Act 2020.

NotifyUs

From 1 December 2020, it became mandatory for organisations to notify the Office of the Privacy Commissioner of any privacy breach that has caused or is likely to cause serious harm to individuals.

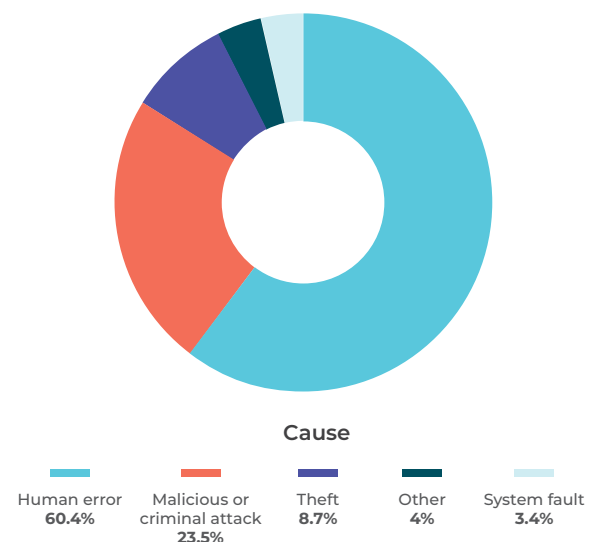
To make it easy for organisations to understand and comply with this new requirement, we worked with business, Government, and not-for-profit representatives to design and build NotifyUs.

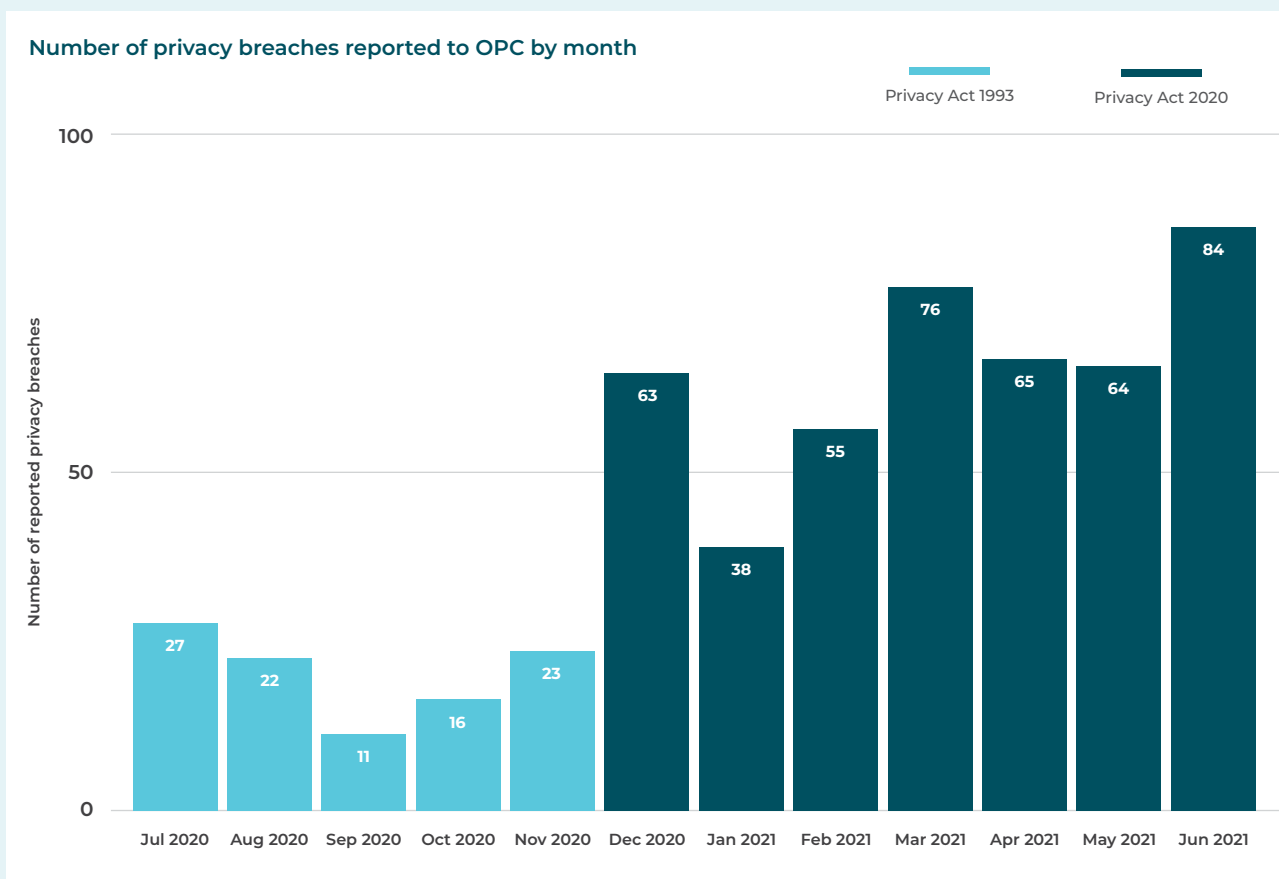
Organisations told us they wanted a tool that gave them confidence about when they need to report a breach and to be able to report in a secure and straightforward way. We needed something that allowed us to effectively manage and respond to the expected increase in notifications and that allowed us to easily identify common causes of serious breaches to inform our education and compliance work.

NotifyUs has two features to make reporting a serious privacy breach easy:

- A *self-assessment tool* where organisations can anonymously complete a short set of questions and be given an immediate response as to whether their privacy breach is likely to meet the threshold for reporting.
- A *reporting tool* that guides agencies through the process of notifying us of a serious breach. The tool allows organisations to easily update information they have provided as they learn more about the breach.

Causes of serious privacy breaches

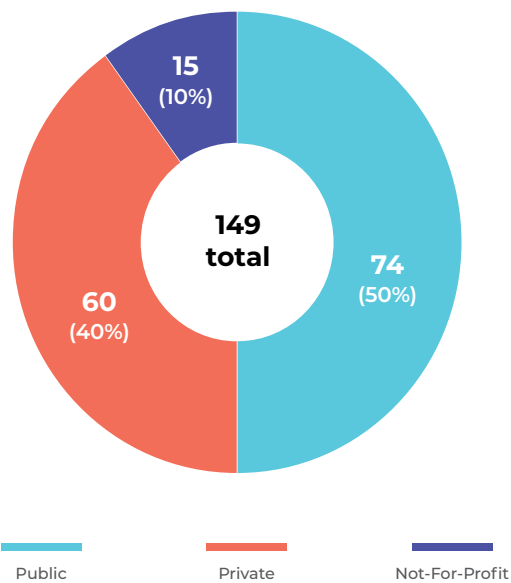




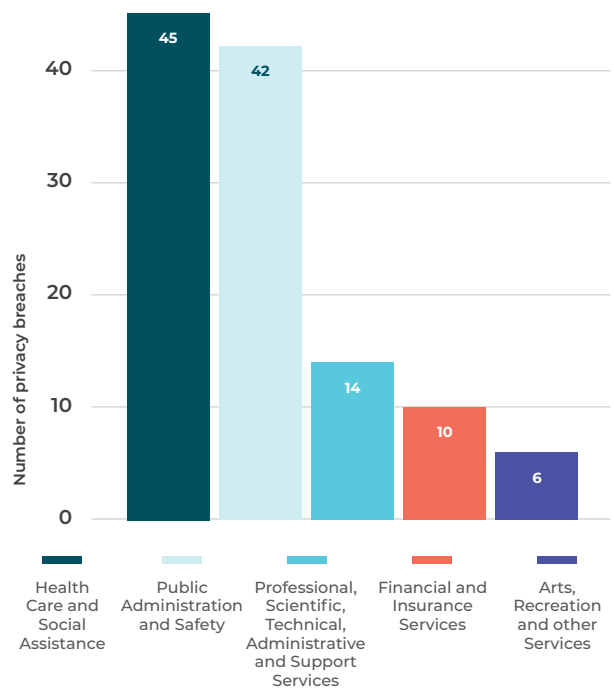
Between 1 December 2020 and 30 June 2021, we received 445 notifications from organisations across the public, private, and not-for-profit sectors through NotifyUs. This was four and a half times the number of notifications we received in the same period the previous year. The standardised reporting format allows us to quickly process the notifications and assist agencies in a timely manner.

NotifyUs provides us with rich data on what types of organisations are reporting privacy breaches, the number of people impacted by these breaches, and the causes of them. We use this data to identify areas where we can target our education or compliance efforts to help prevent breaches. As part of Privacy Week in May 2021, we published data on the key themes from the first four months of reporting along with advice for organisations on how to avoid common issues.

Serious breach notifications by sector



Top five industries reporting serious privacy breaches



NotifyUs was shortlisted as a finalist in the 'Innovation' category of the Global Privacy Assembly's Privacy and Data Protection Awards for 2021.

IPP12 Model Clauses: Protecting New Zealanders' information internationally

The Privacy Act 2020 expanded the information privacy principles from 12 to 13, establishing a new information privacy principle 12. Under IPP12, agencies are now responsible for ensuring that any personal information they send to organisations outside Aotearoa New Zealand is adequately protected.

To make it easy for New Zealand agencies to apply this new principle, we developed new materials to support them.

We released new guidance designed to take agencies through each criterion step by step, providing them with greater certainty as to how they could disclose the personal information.

We also created plain English model contract clauses that organisations can insert into a contract between the New Zealand party and the offshore partner.

Our model contract clauses are tailored to the requirements of the Privacy Act 2020 and are designed to make it easier to comply with principle 12, particularly for small and medium-sized businesses. The clauses can be modified to suit the needs of each individual organisation to ensure that key privacy protections are included in their contracts. These clauses are a resource that can be used by many organisations to help them comply with the new information privacy principle.



Objective 3: OPC is trusted as a fair and responsive regulator

The trust of the people and organisations we serve is central to our effectiveness as a regulator. Citizens need to trust that we are making the best decisions about how to address their privacy needs and concerns, including considering Māori and multicultural perspectives when deciding on the right approach to complaints and enquiries.

Businesses need to feel confident that the OPC is a stable, reliable regulator, and to trust that we will help them meet their privacy obligations while achieving their legitimate commercial objectives. Government needs to trust us to fulfil our role effectively, and to have confidence that we are responsible regulatory stewards.

Our focus in this priority for the year has been in ensuring that agencies and individuals are aware of the approach that we intend to take to enforcing the Privacy Act 2020.

Key to this has been the development and publication of our Compliance and Regulatory Action Framework (CARAF) that sets out how we will approach our regulatory role.

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

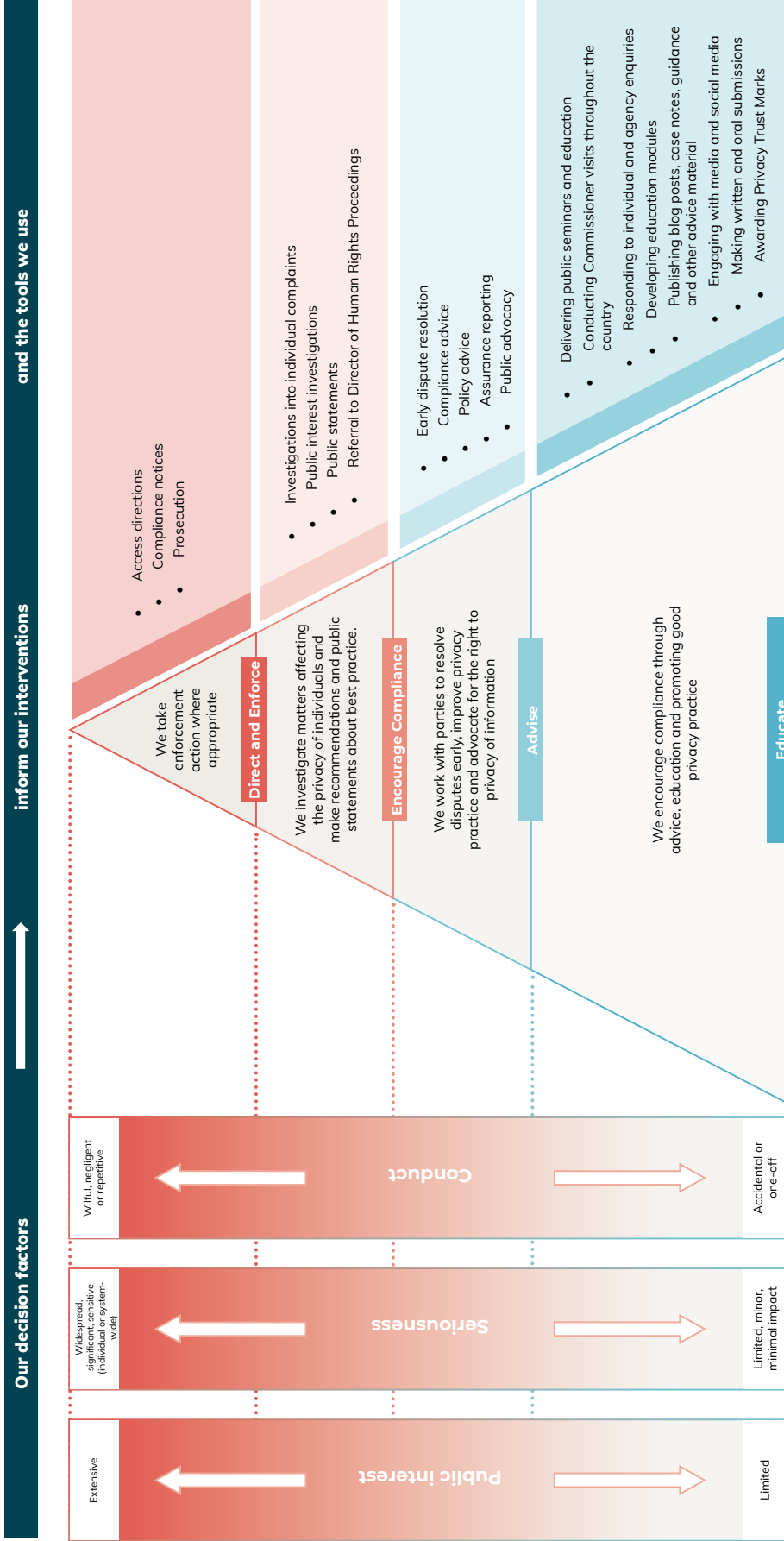
- seriousness or potential impact of a privacy issue on individuals
- the level of public interest in the issue
- the attitude to compliance and conduct of the agency concerned.

Our focus in this priority for the year has been in ensuring that agencies and individuals are aware of the approach that we intend to take to enforcing the Privacy Act 2020.

We set ourselves clear guiding principles that we would use:

- ✓ Fairness
- ✓ Consistency and transparency
- ✓ Proportionality
- ✓ Accountability
- ✓ Kōtuitui (seeking opportunities to partner with Māori whenever possible)

Regulatory Action and Compliance



We were clear in the CARAF that for obligations that came into effect with the new Act, such as mandatory breach notification, we would be focusing on the 'education and awareness' end of our activities for the first three to six months to give agencies an opportunity to prepare to meet their new obligations. Over the first six months of 2021, we supported agencies reporting serious breaches to minimise the harm that these breaches cause to people, and to learn from them so that they don't occur again.

In 2020-2021 we took initial steps in what will be a multi-year journey to embed Te Ao Māori perspectives on privacy. The Privacy Act 2020 requires us to consider cultural perspectives on privacy. In recognition of Te Tiriti o Waitangi, our priority has been building an understanding of a Te Ao Māori perspective and what this means for how we exercise our functions. In this period, we made a start by undertaking a recruitment process for a Principal Adviser Māori, jointly with the Commerce Commission, to lead our work in this area. We also continued upskilling our people in Te Reo Māori and Te Ao Māori by offering Te Reo lessons to all staff and holding an all staff day focused on Aotearoa New Zealand's bicultural roots.

Guidance on 72-hour notification expectation

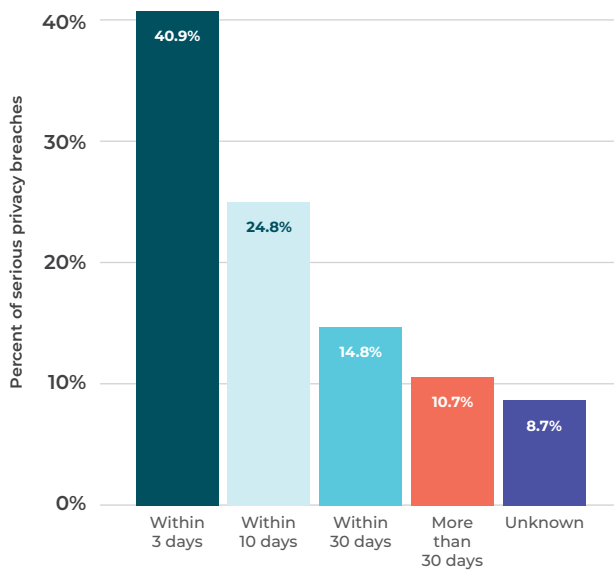
The Privacy Act 2020 requires that agencies notify the Privacy Commissioner and consider notifying affected individuals about any privacy breach that has caused or is likely to cause serious harm to individuals. These breaches include ransomware attacks when personal information is either accessed, stolen, or rendered inaccessible.

The Privacy Act does not specify an exact time limit for when agencies must notify the Privacy Commissioner; instead it states that this must occur 'as soon as practicable after becoming aware that a notifiable privacy breach has occurred.'

In the first few months of the new Act, some agencies were notifying the Commissioner weeks or even months after becoming aware of breaches. Feedback from agencies is that they were unsure of our expectations about how soon to report and were often waiting to gather more information before letting us know of a breach.

As a result of this feedback, we took a more proactive approach to giving agencies clarity about our expectation that, unless there are extenuating circumstances, our Office should be notified of breaches within 72 hours. This requirement is consistent with other leading jurisdictions, such as the European General Data Protection Regulation.

Timeliness of breach reporting to OPC




Timely notification allows us to provide agencies with advice and support as early as possible to ensure that the harm from the breach is minimised.

From complaint to resolution

Our Investigations and Dispute Resolution team are the front line of our Office. They are the first point of contact for the public's privacy enquiries and complaints, and work with a diverse range of complainants and respondents to resolve all manner of complex privacy issues.

In 2020-2021 we closed 580 complaint files. As at 30 June 2021, 16% of the open complaints files had been open for longer than six months. However, the average percentage of open complaints files older than 6 months over the course of the year was only 10%, which is in line with the target set for the year.

We employ external auditors to conduct regular reviews of our investigations. Of the files reviewed this year, 97.5% were rated 3.5 out of 5 or better, exceeding our target of 85%.



90%
The average percentage of open complaints files less than 6 months old during the year



97.5%
of the files reviewed this year were rated 3.5 out of 5 or better, exceeding our target of 85%

Case studies

CASE ONE

Employee browsing

A man who worked for a health agency learned that his mental health records had been accessed by several colleagues with no link to his care. This unauthorised knowledge of his sensitive personal information caused significant emotional impact to his health and work.

Following a complaint to us, we found that the agency had breached its obligations under rules 5 and 11 of the Health Information Privacy Code by not ensuring that sensitive information was kept secure and failing to prevent disclosure to people who had no purpose in seeing it.

We held a conciliation between the man and the agency in which the agency apologised for the harm caused and agreed to support him to continue his employment in a way that minimised the discomfort caused by the breach of his privacy. A payment of \$20,000 was also made to the man, and the agency committed to actions to ensure that other people don't suffer the same harm in future.

Employee browsing like this, where employees access information that they do not need for their job, is a frequent privacy issue. Agencies are required under the Privacy Act 2020 to have systems and processes in place, including appropriate training for their staff, to ensure that employees are only accessing and sharing personal information when required as part of their role.

CASE TWO

CCTV in the workplace

An employee of a pizza parlour complained to us that his workplace had been recording audio on the CCTV cameras on the premises without informing staff or customers. He was concerned that private conversations between staff had been recorded without their knowledge and felt distressed at the thought that they could be accessible to other staff within the business.

Following the lodging of the complaint, the business agreed to stop audio recording. To ensure that the business also had clarity about their obligations under the Privacy Act 2020, we sent them a Compliance Advice Letter setting out the relevant information privacy principles regarding the use of CCTV in the workplace.

Generally, CCTV systems should not record audio if visuals are sufficient because collecting audio significantly increases the privacy intrusiveness. In a workplace setting, sensitive discussions often occur (for example, explaining the reason someone is taking sick leave), and as a result, audio recording is generally regarded as unreasonably intrusive, unless there is a very good reason for its use.

In any use of CCTV, with or without audio recording, signage should be displayed to make it clear to customers and staff what information is being collected, and for what purpose. The footage should be stored securely and only accessed for legitimate purposes.



Objective 4: OPC influences privacy practices and behaviours

The Privacy Act provides us with a range of specific tools to help individuals and promote compliance, but our remit is too large to achieve our mission without the ability to influence organisations and individuals to change their behaviour.

We exert that influence in a range of ways: how we communicate, the cases we choose to take, the outcomes of those cases, and the data we produce to support our positions. Our ability to influence is key to making sure privacy is a central concern for government when it creates and implements policy and law.

Over the course of the year we have continued to be active in seeking to ensure that privacy is central 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 the following law reform or major policy processes:

- consideration of the introduction of a Consumer Data Right
- the Reserve Bank of New Zealand Bill, in relation to provisions which provide the Bank with information-gathering and disclosure powers
- the Protected Disclosures (Whistleblower) Bill, in relation to the protection of the confidentiality of a whistleblower and the application of the Privacy Act
- the Arms (Firearms Prohibitions Orders) Amendment Bill No 2 (a Member's Bill), in relation to the issuing of Firearms Prohibition Orders to gang members who meet certain criteria
- the Rights for Victims of Insane Offenders Bill (a Member's Bill), in relation to the rights of victims of offending by special patients and special care recipients, and potential privacy implications
- Drug and Substance Checking Legislation Bill (No 2) 2021
- Counter-Terrorism Legislation Bill
- International Treaty Examination of the Council of Europe Convention on Cybercrime
- Land Transport (Drug Driving) Amendment Bill
- Films, Videos, and Publications Classification (Urgent Interim Classification of Publications and Prevention of Online Harm) Amendment Bill
- Harmful Digital Communications (Unauthorised Posting of Intimate Visual Recording) Amendment Bill
- Proposals for Approved Information Sharing Agreements.

Over the course of the year we have continued to be active in seeking to ensure that privacy is central when policy and law is being developed.

Nationwide media campaign: 'Privacy is Precious'

The Privacy Act 2020 provided an opportunity to ensure that both organisations and individuals were aware of their rights and responsibilities when providing and collecting personal information.

A survey conducted in 2020 (before the new Act) found that only 37% of respondents felt their information was protected under the current law, and only 18% felt in control of how businesses use their information.

In November and December 2020, the Office of the Privacy Commissioner commissioned its first advertising campaign to promote understanding of the changes to the Act as well as general awareness of privacy.

The 'Privacy is Precious' campaign focused on groups who have historically been less engaged with the Office, including Māori and Pasifika, small businesses, not-for-profit and community organisations, and the real estate sector. It used a range of channels like television, digital video, radio, social media, digital displays, search targeting, and sponsored print and digital content.

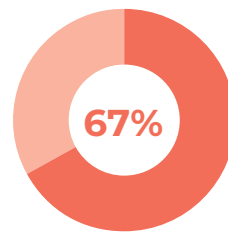
The combination of channels enabled the campaign to reach a significant portion of the Aotearoa New Zealand public at least once, including two-thirds of all people aged 25-64, and 52% of all Māori and Pasifika aged 18-64. This means that about 1.62 million New Zealanders saw a campaign ad an average of six times over the course of the six-week campaign. Visitors to the campaign landing page spent an average of more than ten minutes on the page.

'Privacy is Precious' ads, videos, resources, and other content were designed to be enduring resources for individuals and businesses seeking information about their privacy rights and responsibilities. There were more than 57,000 visits to the landing page during the six-week campaign.

Campaign metrics including click through rates, visits, and time spent all exceeded industry averages, demonstrating public interest in learning more about privacy and suggesting that the campaign successfully raised awareness of the changing Act and new obligations for organisations.

The changes to the Privacy Act 2020 marked an exciting opportunity for the Office of the Privacy Commissioner to reach new audiences and engage more meaningfully with our existing stakeholders.

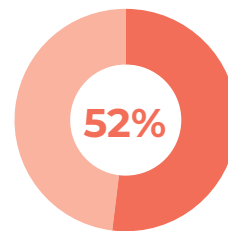
The 'Privacy is Precious' campaign focused on groups who have historically been less engaged with OPC, including Māori and Pasifika, small businesses, not-for-profit and community organisations, and the real estate sector.



The campaign reached 67% of all people aged 25-64 years

1.62m

People reached



The campaign reached 52% of all Māori and Pasifika aged 18-64

Supporting the public health response to COVID-19

Throughout 2020-2021 the Government developed a range of initiatives to manage Aotearoa New Zealand's response to the COVID-19 pandemic, many of which have involved the collection, use, or disclosure of personal information.

Our policy advice to Government has encouraged the development of policies to only use personal information when it is necessary and in proportion to the problem being addressed.

We provided policy advice across a range of COVID-19 related policies to support Aotearoa New Zealand's response to the pandemic, as well as advice direct to the public via our website. Our focus has been on ensuring all policy is developed with 'privacy by design' principles at the forefront.

All COVID-19 response initiatives with a privacy impact should be based on a clear and demonstrated public health need to maintain public trust and confidence in the response.

Our work has included privacy-related advice on:

- COVID-19 Vaccination Certificates
- mandatory record keeping and contact tracing
- updates to the COVID-19 Tracer App
- managed isolation and quarantine facilities, including the self-isolation pilot
- vaccines and the workplace
- COVID-19 response legislation and Orders
- the serious threat to public health exception in the Privacy Act and its application in the context of COVID-19.



Shaping practice in the rental sector

As part of our process of gathering intelligence about privacy practice across sectors, it came to our attention that large amounts of information were being collected from prospective tenants seeking rental accommodation.

Demand for rental accommodation across Aotearoa New Zealand has led to prospective tenants competing for fewer properties, making them vulnerable to requests for personal information that go beyond what is necessary for assessing their suitability for a tenancy.

In 2020-2021 we prioritised engaging with tenants and landlords to get a good understanding of practice in the rental market – what is being collected and how it is being used and cared for. Both tenants and landlords told us that they needed more certainty about what is acceptable in terms of the collection and use of personal information. This sector remains a priority into the 2021-22 year when we will provide guidance to landlords and tenants and look to monitor privacy practice in the sector.

In 2020-2021 we prioritised engaging with tenants and landlords to get a good understanding of privacy practice in the rental market – what is being collected and how it is being used and cared for.



Office and functions



Independence and functions

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 and public interests.

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

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

Reporting

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

Staff

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

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

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

The COVID-19 pandemic has continued to affect the Office and functions of the Privacy Commissioner during the year to 30 June 2021.

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 Office 365 software for operational matters and an electronic document records management system so staff can securely access records remotely.

Remote working is further supported by video conferencing via Zoom to facilitate interaction across all staff, and with outside parties when required.

EEO profile

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 continued to be:

- developing talent regardless of gender, ethnicity, age, or other demographic factors
- integrating work practices that promote or enhance work/life balance amongst employees, including family-friendly practices
- maintaining equitable, gender-neutral remuneration policies that 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 advertising, 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 2021

Role	Women		Men		Total
	Full-time	Part-time	Full-time	Part-time	
Commissioner			1		1
Senior managers	2	1	1		4
Team and unit managers	3	1	2		6
Investigations and Dispute Resolution	3	2	3		8
Administrative support	5	2	1		8
Policy	3		2	1	6
Compliance and Enforcement	2	1	1		4
Strategy and Communications		1	1	1	3
Legal	1	1	1		3
Total	19	9	13	2	43

Finance and performance report



Statement of responsibility

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

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

The Privacy Commissioner has 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 2021.



J C Edwards
Privacy Commissioner
20 December 2021



G F Bulog
General Manager
20 December 2021

Statement of performance

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

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

Our Statement of Intent 2020-2024 identifies four high level objectives to support our mission to be an “effective modern privacy regulator”. The previous sections of this Annual Report provide evidence on how the Office has performed against each of these objectives during the year.

The Statement of Performance Expectations for the year to June 2021 identified five new output areas (Primary Activities) to support these four objectives. The new and extended responsibilities set out in the Privacy Act 2020 provided an opportunity to change the operational and functional design of the Office.

We report our progress against these Primary Activities in this section and have linked 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

The impact of the COVID-19 emergency on the ability of the Office to deliver its key services up to 30 June 2021 was limited. Staff were able to work from home and service delivery continued across the Office.

Reliable data and information was available in order to report against all measures, and despite the COVID-19 emergency, 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 continue to regularly monitor this risk.

Statement specifying comprehensive income

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

Specified comprehensive income	Target \$000	Achievement \$000
Operating grant	7,276	7,276
Other revenue	236	259
Total revenue	7,512	7,535

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 1.9% of the total Vote Justice Non-Departmental Output Expenses Appropriation for 2020/21. The total expenses in the year are \$7,050k as set out in the cost of service statement below.

Cost of service statement

for the year ended 30 June 2021

As set out in the 2020/21 Statement of Performance Expectations, the Privacy Commissioner committed to provide five primary activities. This is an increase on previous years where there were only four and represents the new and extended responsibilities of the Office set out in the Privacy Act 2020. The 2020 split has been re-stated to show where costs would now sit. The split of funds across these five primary activities is set out below:

	Actual 2021 \$000	Budget 2021 \$000	Actual 2020 restated \$000
PRIMARY ACTIVITY 1: COMMUNICATION AND EDUCATION			
Resources employed			
Revenue	768	919	924
Expenditure	871	937	865
Net Surplus/(Deficit)	(103)	(18)	59
PRIMARY ACTIVITY 2: ADVICE AND ADVOCACY			
Resources employed			
Revenue	1,196	1,179	2,230
Expenditure	1,112	1,191	2,283
Net Surplus/(Deficit)	84	(12)	(53)
PRIMARY ACTIVITY 3: COMPLIANCE AND ENFORCEMENT¹			
Resources employed			
Revenue	1,975	1,904	778
Expenditure	1,732	1,841	669
Net Surplus/(Deficit)	243	63	109
PRIMARY ACTIVITY 4: INVESTIGATION AND DISPUTE RESOLUTION			
Resources employed			
Revenue	1,727	1,618	2,099
Expenditure	1,491	1,560	2,094
Net Surplus/(Deficit)	236	58	5

¹ This is a new primary activity. In the budget this included all the Information Sharing and Matching related costs. The prior year comparative therefore includes all the associated costs under the previously named Information Sharing and Matching output class.

	Actual 2021 \$000	Budget 2021 \$000	Actual 2020 restated \$000
PRIMARY ACTIVITY 5: STRATEGY AND INSIGHTS²			
Resources employed			
Revenue	1,869	1,892	–
Expenditure	1,844	1,955	–
Net Surplus/(Deficit)	25	(63)	–
TOTALS			
Resources Employed			
Revenue	7,535	7,512	6,031
Expenditure	7,050	7,484	5,911
Net Surplus/(Deficit)	485	28	120

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

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



² This is a new primary activity. There were no costs associated with this area in 2020 and therefore no comparatives.



Primary activity 1: Strategy and insights

Activity areas of focus

- Understanding our trends and technological developments will be relevant in the future.
- Using evidence based on all the inputs, including complaints, media, breach reporting, enquiries, international regulators or website analytics, to prioritise work and make decisions.
- Monitoring 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 2020/21	Achieved 2019/20
Quantity			
Number of interventions analysed. 	10	Not achieved – 4 An initial analysis of the trends on the Office's operational intelligence was conducted in late 2020 and used as input into selecting three cross-Office strategic priorities for the first half of 2021. Action plans were developed for each of the priorities and progress was monitored by a newly established office panel. In addition, an insights piece that provided data on the first four months of mandatory privacy breach reporting was published in May 2021. At the year-end, work on the three priorities noted above was still ongoing and as a result the Office had not yet measured the effectiveness.	Not applicable – new measure in 2020-2021.
Number of interventions considered effective. 	85%	At the year-end, work on the priorities noted above was still on-going and as a result the Office had not yet measured the effectiveness.	Not applicable – new measure in 2020-2021.




Measure	Estimate	Achieved 2020/21	Achieved 2019/20
Quality and timeliness			
<p>Work is focused on globally identified privacy trends and new emerging technologies.</p> 	5	<p>Achieved – 5</p> <p>The Office continues to monitor international developments around digital identity and emerging technology and is actively involved in the development of the digital identity ecosystem in Aotearoa New Zealand.</p> <p>During the year, the Office undertook work in the following areas:</p> <ul style="list-style-type: none"> • Biometrics • COVID-19 contact tracing solutions • Digital Identity Trust Framework • Cross border information flows • Strengthening privacy protections in legislation 	Not applicable – new measure in 2020-2021.
<p>Systems for monitoring and reporting on the progress of new strategies are fit for purpose.</p> 	100%	<p>A new organisational structure to support the Office to take a proactive and strategic approach to its work under the new legislation went live at the end of October 2020.</p> <p>A new panel was set up to help identify, drive, and monitor the effectiveness of the Office priorities and to oversee the implementation of these first three cross-office priorities.</p> <p>Systems continue to be reviewed and developed internally to systemise the Office's use of business intelligence to support prioritisation.</p>	Not applicable – new measure in 2020-2021.

Primary activity 2: Communications and education

Activity areas of focus

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




Output Measures

Measure	Estimate	Achieved 2020/21	Achieved 2019/20
Quantity			
Number of people completing education modules on the online system. ³ 	5,000	Achieved 51,679 people have completed e-learning modules in the year to 30 June 2021. The significant increase is mainly due to the new modules introduced in the year relating to Privacy Act 2020.	Achieved – 12,725
Presentations at conferences and seminars. ⁴ 	100	Achieved – 151 An increase in virtual conferences due to COVID-19 precautions allowed the Office to participate in more events.	Substantially achieved – 89
Public enquiries received and answered. ⁵ 	8,500	Achieved – 9,165 Public enquiries are externally driven and will fluctuate between years.	Not Achieved – 7,734

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.

4 As per footnote 3 but the expectation differed from the SPE and was 90.

5 As per footnote 3.

Measure	Estimate	Achieved 2020/21	Achieved 2019/20
Quantity			
Percentage uptake on media comments made by the Office. ⁶ 	95%	Achieved 293 media enquiries were received. 95% of these were responded to with a substantive comment or information provided by the Office.	Not applicable – new measure in 2020-2021.
Quality and timeliness			
The office actively engages in and has proactively established multi-stakeholder relationships both nationally and internationally. 	90% ⁷	Achieved The Office has continued to be actively engaged with its international co-regulators during the period. Domestically, the Office has continued to engage with peak industry bodies and stakeholders around the implementation of the new Privacy Act.	Achieved Despite the impacts of COVID-19, we continued our engagement both nationally and Internationally. See the Outreach section for further information.
Respond to all enquiries within two working days. ⁸ 	95%	Substantially achieved – 90%	Substantially achieved – 93%

6 As per footnote 3.

7 The measure was intended to be qualitative rather than quantitative. The target of 90% set in the SPE does not best represent the measure. This measure has been removed from the 2022 SPE.




8 As per footnote 3.

Primary activity 3: Compliance and enforcement




Activity areas of focus

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

Output Measures

Measure	Estimate	Achieved 2020/21	Achieved 2019/20
Quantity			
Number of data breach notifications received. ⁹ 	800	Not achieved – 544 469 of these were received through the new NotifyUs system which went live in November 2020. Breach notifications are externally driven and will fluctuate between years.	Achieved – 205
Compliance Notices raised where necessary. 	6	Not achieved No compliance notices were raised in the year to 30 June.	Not applicable – new measure in 2020-2021.
The number of proposals consulted on involving information sharing or matching between government agencies completed during the year. 	30	Not achieved – 11	Not achieved – 22

⁹ As per footnote 3. This target was added as part of the Supplementary Estimates process.

Measure	Estimate	Achieved 2020/21	Achieved 2019/20
Quality and timeliness			
Targeted guidance is provided to agencies and follow up reviews are undertaken where necessary. 	95% ¹⁰	Achieved The first six months of the 2020 Act (Jan to June 2021) were focused on education and guidance. From 1 June, the Office moved to a more compliance focus and issued six formal warnings during the month along with advice and guidance. No formal follow-up reviews were undertaken.	Not applicable – new measure in 2020-2021.
Issues identified as a strategic priority result in timely and focused action plans. 	Achieved	Achieved Work continued on each of the first three cross-office priorities in the period to 30 June. Action plans were developed for each of these priorities and progress was monitored.	Not applicable – new measure in 2020-2021.
The percentage of externally reviewed policy, information sharing and matching files that are rated as 3.5 out of 5 or better for quality. ¹¹ 	85%	Achieved – 85%	Achieved – 89%

¹⁰ The measure was intended to be qualitative rather than quantitative. The target of 95% set in the SPE does not best represent the measure. This measure has been removed from the 2022 SPE.

¹¹ As per footnote 3.



Primary activity 4: Advice and advocacy

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 perspective and recognises risks and competing interests.
- Effective intervention including the development of privacy codes and advice to government on changes to other legislation.
- Advocating for privacy positive outcomes, including privacy by design.

Output Measures

Measure	Estimate	Achieved 2020/21	Achieved 2019/20
Quantity			
The number of consultations, submissions, office projects completed in the year. 	150	Not achieved – 117 The number of consultations is demand driven through external organisations.	Achieved – 151
The number of formal reports produced that relate to information sharing or information matching programmes, under the Privacy Act. 	8	Not achieved – 1	Not achieved – 4

Measure	Estimate	Achieved 2020/21	Achieved 2019/20
Quality and timeliness			
<p>Advice provided to Government on other legislation has a positive impact.</p> 	90% ¹²	<p>The policy function has continued to prioritise the response to COVID-19.</p> <p>The Office's advice has had a positive impact, including meaningful advice provided on key COVID-19 response initiatives, that significantly reshaped the final proposal.</p> <p>In addition, the Office continued to provide submissions on key bills, positively influencing the shape of the final legislation passed.</p>	Not applicable – new measure in 2020-2021.
<p>International engagement and activities have a positive impact in the realisation of privacy rights.</p> 	100% ¹³	<p>The Office has been represented, and has contributed at global and regional networks such as the Global Privacy Assembly, OECD, APEC Data Subgroup (APEC DPS), and the Asia Pacific Privacy Authorities (APPA) Forum to ensure it had a positive impact on privacy issues globally and throughout the year.</p> <p>The Office has actively continued to contribute to international discussions on COVID-19 related privacy matters, and participated in the OECD working group on trusted government access, and the APPA Forum.</p>	Not applicable – new measure in 2020-2021.

¹² The measure was intended to be qualitative rather than quantitative. The target of 90% set in the SPE does not best represent the measure. This measure has been removed from the 2022 SPE.




¹³ The measure was intended to be qualitative rather than quantitative. The target of 100% set in the SPE does not best represent the measure. This measure has been removed from the 2022 SPE.

Primary activity 5: Investigations and dispute resolution

Activity areas of focus





- Working with parties to achieve a fair outcome using dispute resolution techniques in the first instance.
- Investigating individual complaints where dispute resolution is inappropriate or unsuccessful.
- Declining to investigate cases where investigations are unnecessary or inappropriate.
- Referring serious cases to the Director Human Rights Proceedings and issuing compliance notices and access directions.

Output Measures

Measure	Estimate	Achieved 2020/21	Achieved 2019/20
Quantity			
Number of complaints received and investigated. ¹⁴  	800	Not achieved 561 complaints were received in the year to 30 June. Of these, 375 (67%) had been notified. In addition, there were 14 files which were not notified but where a Compliance Advice Letter was sent during the year. Complaint numbers are externally driven and will fluctuate between years.	Not achieved – 691
Percentage of investigations discontinued based on assessments against defined criteria. ¹⁵ 	15%	48% of files closed since 1 December 2020 were discontinued. This represents 149 files (excluding files with no substance) out of a total closed of 311 since December.	Not applicable – new measure in 2020-2021.

¹⁴ As per footnote 3.

¹⁵ This measure reflects the use of new powers under the legislation to discontinue investigations on criteria defined by the Privacy Commissioner.

Measure	Estimate	Achieved 2020/21	Achieved 2019/20
Quality and timeliness			
The percentage of complaints files closed by settlement between the parties. ¹⁶ 	40%	Achieved – 65%	Achieved – 64%
The percentage of externally reviewed complaints investigations that are rated as 3.5 out of 5 or better for quality. ¹⁷ 	85%	Achieved – 97.5% Based on the results of an external review of a sample of complaints files closed between July 2020 and June 2021.	Achieved – 95%
The average percentage of open complaints files greater than 6 months old during the year. ¹⁸ 	10%	Achieved – 10%	Not applicable – new measure in 2020-2021.
The percentage of open files greater than 6 months old at the year-end. ¹⁹ 	10%	Not achieved – 16%	Not achieved – 11%

¹⁶ As per footnote 3.

¹⁷ As per footnote 3.

¹⁸ This target has changed slightly from the prior year when the KPI was only based on the aging as at 30 June rather than an annual average (see footnote below). For comparative purposes the result in the prior year would have been 14%.

¹⁹ This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation. It was amended in the final SPE as per the measure above but not amended in the Supplementary Estimates. It was reported against in the 2020 Annual Report as shown.

Statement of accounting policies

for the year ended 30 June 2021

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 2021 and were approved by the Commissioner on 20 December 2021. 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 the New Zealand Dollar.

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 percent 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, other than that there are now 5 separate cost areas compared to 4.

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 2021:

- Lease classification – refer Note 4
- Non-government grants – refer Note 2
- Grant expenditure – refer Note 4

Statement of comprehensive revenue and expenses

for the year ended 30 June 2021

	Note	Actual 2021 \$000	Budget 2021 \$000	Actual 2020 \$000
Revenue				
Crown revenue	2	7,276	7,276	5,708
Other revenue	2	259	236	323
Total income		7,535	7,512	6,031
Expenditure				
Promotion	4	580	209	124
Audit fees		33	33	33
Depreciation and amortisation	4,8,9	235	219	201
Rental expense		450	408	396
Operating expenses	4	1,230	1,125	891
Contract services		373	398	648
Staff expenses	3	4,149	5,092	3,618
Total expenditure		7,050	7,484	5,911
Surplus/(Deficit)		485	28	120
Other comprehensive revenue and expenses		-	-	-
Total comprehensive revenue and expenses		485	28	120

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

for the year ended 30 June 2021

	Note	Actual 2021 \$000	Budget 2021 \$000	Actual 2020 \$000
Total equity at the start of the year		1,096	690	976
Total comprehensive revenue and expenses for the year		485	28	120
Total equity at the end of the year	5	1,581	718	1,096

Explanations of major variances are provided in Note 1.

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

Statement of financial position

as at 30 June 2021

	Note	Actual 2021 \$'000	Budget 2021 \$'000	Actual 2020 \$'000
Public equity				
General funds	5	1,581	718	1,096
Total public equity		1,581	718	1,096
Current assets				
Cash and cash equivalents	6	1,272	502	1,093
Receivables	7	80	34	187
Prepayments	7	115	50	105
Inventory		-	15	-
Total current assets		1,467	601	1,385
Non-current assets				
Property, plant, and equipment	8	293	237	204
Intangible assets	9	333	233	109
Capital work in progress	8,9	115	-	82
Total non-current assets		741	470	395
Total assets		2,208	1,071	1,780
Current liabilities				
Payables	10	205	150	338
Employee entitlements	12	400	180	317
Total current liabilities		605	330	655
Non-current liabilities				
Lease incentive	11	22	23	29
Total non-current liabilities		22	23	29
Total liabilities		627	353	684
Net assets		1,581	718	1,096

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

Statement of cash flows

for the year ended 30 June 2021

	Actual 2021 \$000	Budget 2021 \$000	Actual 2020 \$000
CASH FLOWS FROM OPERATING ACTIVITIES			
Cash was provided from:			
Receipts from the Crown	7,276	7,276	5,708
Receipts from other revenue	394	212	179
Interest received	1	24	11
Cash was applied to:			
Payment to suppliers	2,743	2,195	2,033
Payments to employees	4,067	5,094	3,521
Net Goods and Services Tax	30	(11)	1
Net cash flows from operating activities	831	234	343
CASH FLOWS FROM INVESTING ACTIVITIES			
Cash was applied to:			
Purchase of property, plant, and equipment and intangibles	652	255	90
Cash was provided from:			
Sale of property, plant, and equipment and intangibles	–	–	–
Net cash flows from investing activities	652	255	90
Net increase/(decrease) in cash held	179	(21)	253
Plus opening cash	1,093	523	840
Closing cash balance	1,272	502	1,093
Cash and bank	1,272	502	1,093

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

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

Notes to the financial statements

for the year ended 30 June 2021

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 \$457k. This is primarily due to the following:

Staff expenses (down on budget by \$943k)

The budget included several new positions as a result of the new functions and responsibilities under the Privacy Act 2020. Delays in recruiting to a number of these positions, in addition to some staff departures and vacancies in other areas, resulted in the expenses being far lower than anticipated.

Promotion costs (up on budget by \$371k)

To assist in implementing the new Privacy Act, the Office undertook its "Privacy is Precious" campaign towards the end of 2020. This was a significant awareness and advertising campaign that ran across television, radio, and other digital channels. It was the first nationwide campaign carried out to raise awareness about privacy and achieved a high reach across a range of communities.

Rental expenses (up on budget by \$42k)

During the year, the Wellington office lease expired and a new lease was negotiated for a different location. The short overlap in these leases resulted in costs being over budget.

Other operating expenses

The three main areas which are over budget for the year are computer maintenance costs (over by \$112k), recruitment (over by \$108k), and repairs and maintenance (over by \$105k). The increase in computer costs is mainly due to the monthly plan costs coming in higher than budgeted. The recruitments costs are due to the large number of new roles that were created and recruited for throughout the year, coupled with a number of staff departures.

The repairs and maintenance overspend is due to the costs associated with the "make good" clause being invoked for the previous Wellington office.

In addition, there were several areas that are below budget. The most significant were litigation and travel. This accounts for \$232k.

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 its 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.

Sales of publications

Sales of publications are recognised when the product is sold to the customer.

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 (2020: \$nil).

Other revenue breakdown

	Actual 2021 \$000	Actual 2020 \$000
Other grants received	161	161
Forums and conferences	19	-
Other revenue	78	151
Interest revenue	1	11
Total other revenue	259	323

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 2021 \$000	Actual 2020 \$000
Salaries and wages	3,917	3,384
Employer contributions to defined contribution plans	114	101
Other staff expenses	36	36
Increase/(decrease) in employee entitlements	82	97
Total staff expenses	4,149	3,618

Employees' remuneration

The Office of the Privacy Commissioner is a Crown entity and is required to disclose certain remuneration information in its annual reports. The information reported is the number of employees receiving total remuneration of \$100,000 or more per annum. The table below has been produced in \$10,000 bands to preserve the privacy of individuals.

Total remuneration and benefits	Number of employees	
	Actual 2021	Actual 2020
\$100,000 – \$109,999	5	3
\$110,000 – \$119,999	2	1
\$120,000 – \$129,999		1
\$130,000 – \$139,999		1
\$140,000 – \$149,999	1	2
\$150,000 – \$159,999	2	1
\$160,000 – \$169,999		
\$170,000 – \$179,999	1	2
\$180,000 – \$189,999		
\$190,000 – \$199,999		
\$330,000 – \$339,999	1	
\$340,000 – \$349,999		1

During 2020-2021, payments in relation to cessation were made to one employee totalling \$18,333 (2020: \$nil).

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

Commissioner's total remuneration

In accordance with the disclosure requirements of section 152(1)(a) of the Crown Entities Act 2004, the total remuneration includes all benefits paid during the period 1 July 2020 to 30 June 2021. As a result of COVID-19, the Commissioner took a pay reduction for part of the year.

Name	Position	Amount 2021	Amount 2020
John Edwards	Privacy Commissioner	335,568	346,000

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 year. A total of \$11k was expensed in relation to these grants in 2021 (2020: \$62k).

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 2021 \$000	Actual 2020 \$000
Fees paid to auditors:		
External audit – current year	33	33
Promotion costs:		
Website development expenses	109	96
Privacy Forum	17	–
Conferences	–	–
Other marketing expenses	454	28
Total promotion expenses	580	124
Depreciation and amortisation:		
Furniture and fittings	59	90
Computer equipment	39	33
Office equipment	9	9
Intangibles	128	69
Total depreciation and amortisation	235	201
Rental expense on operating leases	450	396
Contract services	373	648
Other operating expenses:		
Computer maintenance/licences	320	281
Staff travel	48	120
Staff development	48	33
Loss on disposal	31	–
Grant expenditure	11	62
Recruitment	192	18
Utilities	251	209
Other	329	168
Total other operating expenses	1,230	891

Operating leases as lessee

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

	Actual 2021 \$000	Actual 2020 \$000
Not later than one year	426	317
Later than one year and not later than five years	1,589	549
Later than five years	141	58
Total non-cancellable operating leases	2,156	924

The Privacy Commissioner leases two properties, one in Wellington and the other in Auckland. The old Wellington lease expired in February 2021 and a new lease commenced on 1 January 2021 for a period of 6 years. The current 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 2021 \$000	Actual 2020 \$000
Opening balance	1,096	976
Net (deficit)/surplus	485	120
Closing balance	1,581	1,096

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 2021 \$000	Actual 2020 \$000
Cash on hand and at bank	54	243
Cash equivalents – on call account	1,218	850
Total cash and cash equivalents	1,272	1,093

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 2021 \$000	Actual 2020 \$000
Receivables	80	187
Prepayments	115	105
Total	195	292
Total receivables comprise:		
GST receivable (exchange transaction)	80	51
Other receivables (non-exchange)	–	136
Total	80	187

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 (2020: \$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.

Critical accounting estimates and assumptions

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

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

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

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

- physical inspection of assets
- asset replacement programmes
- review of second-hand market prices for similar assets
- 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 2019	785	164	76	1,025
Additions	27	23	1	51
Disposals	(297)	–	–	(297)
Balance at 30 June 2020	515	187	77	779
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
Accumulated depreciation and impairment losses				
Balance at 1 July 2019	627	78	35	740
Depreciation expense	90	33	9	132
Elimination on disposal	(297)	–	–	(297)
Balance at 30 June 2020	420	111	44	575
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
Carrying amounts				
At 30 June 2020	95	76	33	204
At 30 June 2021	188	80	25	293

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 \$72k as at 30 June 2021 (2020: \$nil). This related to work in the Wellington office.

Work in progress

The capital work in progress figure is \$11k as at 30 June 2021 (2020: \$nil). This all related to work undertaken in the Wellington office.

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.

Critical accounting estimates and assumptions

Estimating useful lives of software assets

The Office's capitalised interactive website tools comprise of a number of interactive website tools and e-learning modules that have been capitalised over the past 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

The IASB's Interpretations Committee issued an agenda decision during April 2021 that clarifies the accounting treatment expected under International Financial Report Standards for customisation and configuration costs associated with software as a service (SAAS) arrangements. The PBE IPSAS-based standards do not provide specific guidance on SAAS arrangements. However, PBE IPSAS 3 explains that in the absence of a PBE standard specifically dealing with a transaction, management may consider the most recent pronouncements of other standards setting bodies. An example of such pronouncements includes interpretations issued by the IASB's Interpretations Committee. As at 30 June 2021, the Privacy Commissioner has recorded an intangible asset of \$222,894 related to SAAS arrangements. The Privacy Commissioner is currently assessing how the principles of the agenda decision could be applied to its SAAS arrangements. Due to the material amount of costs involved that have been incurred over several years and the judgements required, the Privacy Commissioner has not had sufficient time to fully consider this. Any changes to our historical accounting treatment will be accounted for as a change in accounting policy in our next financial statements for the year ended 30 June 2022.

In addition to the \$222,894 noted above, there is a remaining amount of capitalised website interactive tools currently assessed as not meeting the definition of a SAAS and therefore not included in this total.

Movements for each class of intangible asset are as follows:

	Acquired software \$000	Interactive tools \$000	Total \$000
Cost			
Balance at 1 July 2019	133	243	376
Additions	12	15	27
Disposals	–	–	–
Balance at 30 June 2020	145	258	403
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	159	596	755
Accumulated amortisation and impairment losses			
Balance at 1 July 2019	29	196	225
Amortisation expense	41	28	69
Disposals	–	–	–
Balance at 30 June 2020	70	224	294
Balance at 1 July 2020	70	224	294
Amortisation expense	44	84	128
Disposals	–	–	–
Balance at 30 June 2021	114	308	422
Carrying amounts			
At 30 June and 1 July 2020	75	34	109
At 30 June 2021	45	288	333

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 \$10k as at 30 June 2021 (2020: \$122k). This all relates to the on-line complaints tool, some of which was included in Work in Progress as at 30 June 2021.

Work in progress

The Capital Work in Progress figure for 2021 is \$103k (2020: \$82k). Most of these costs are associated with the development of the new online Complaints tool.

Note 10: Payables

Accounting policy

Creditors and other payables are recorded at the amount payable.

Breakdown of payables

	Actual 2021 \$000	Actual 2020 \$000
Payables under exchange transactions		
Creditors	149	208
Accrued expenses	50	112
Lease incentive	7	18
Total payables under exchange transactions	205	338
Payables under non-exchange transactions		
Other payables	-	-
Total payables under non-exchange transactions	-	-
Total creditors and other payables	205	338

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 2021 \$000	Actual 2020 \$000
Lease incentive	22	29
Total non-current liabilities	22	29

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 2021 (2020: \$nil).

Breakdown of employee entitlements

	Actual 2021 \$000	Actual 2020 \$000
Current employee entitlements are represented by:		
Accrued salaries and wages	139	86
Annual leave	261	232
Total current portion	400	317
Current	400	317
Non-current	-	-
Total employee entitlements	400	317

Note 13: Contingencies

There are no known contingencies existing at balance date (2020: \$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 part 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 2021	Actual 2020
Total salaries and other short-term employee benefits (\$000)	981	926
Full-time equivalent members	4.6	4.3

Key management personnel include all senior managers and the Privacy Commissioner who together comprise the Senior Leadership Team (SLT). One member of the SLT left during the year, one member was replaced part way through the year and a new senior manager position was filled towards the end of the 2020 calendar year.

Note 15: Post balance date events

As a result of COVID-19, during August 2021 the alert levels across Aotearoa New Zealand increased resulting in a period of lockdown. This has not impacted the financial results as shown.

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:

	2021 \$000	2020 \$000
FINANCIAL ASSETS		
Financial assets measured at amortised cost		
Cash and cash equivalents	1,272	1,093
Receivables (excluding prepayments and taxes receivables)	0	136
Total loans and receivables	1,272	1,229
FINANCIAL LIABILITIES		
Financial liabilities at amortised cost		
Payables (excluding income in advance, taxes payable, grants received subject to conditions and lease incentive)	199	320
Total financial liabilities at amortised cost	199	320

Note 17: COVID-19 financial impact assessment

Impact of COVID-19

During August and September 2020 and February and March 2021, the Auckland region moved to Alert Levels 3 and 2, and other parts of the country moved to Alert Level 2. Towards the end of June 2021, the Wellington region moved to Alert Level 2 for one week. Subsequent to balance date, the levels have continued to move as noted in Note 15.

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 3. This had limited impact on the Office's ability to deliver key services due to a previous IT infrastructure update to enable staff to work remotely.

Revenue

There was no impact on Crown Revenue.

Expenditure

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

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.

After a review, we believe there is no impairment on the collectability of these debtors caused by COVID-19.

There are no other significant assumptions being made concerning the future and no other key sources of estimation uncertainty at the reporting date that pose significant risk of causing material adjustments to the carrying balances of assets and liabilities within the next financial year.

Appendices



Appendix A

Processes and services

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 breaches a privacy principle and causes 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 assess 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 someone's 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. During the 2020-2021 year, there were no referrals to the Director of Human Rights Proceedings.

In some cases, the team will decline to investigate where an investigation would be unnecessary or inappropriate. They will endeavour to provide people with the reasons why they cannot investigate, and if they can, refer the complainant to another agency that may 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 public 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 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 monitoring information sharing and matching by government agencies. Information sharing and matching raises several privacy issues, such as the potential to disclose incorrect information or the potential to 'automate away' human judgment.

There are two monitoring regimes

Approved Information Sharing Agreements (AISAs) are agreements between government agencies, authorised by regulation, that allow them to share information with one another.

We are consulted on these agreements and highlight potential risks. Agencies are obliged to report their activity on their websites. Our complaints and enforcement functions apply to AISA breaches.

Authorised Information Matches are agreements between government agencies, authorised by legislation, that allow them to share information with one another.

The Commissioner's functions include reporting to Parliament annually with an assessment of each programme's compliance with the Privacy Act, and reviewing and reporting on each legislative provision within a 5-year cycle.

Communications and engagement

Our primary purpose is to provide New Zealanders with the knowledge and resources they need to protect their privacy, and to ensure agencies have the information they need to meet their obligations. This requires us to:

- build partnerships and relationships with organisations that can help us increase our impact
- understand the privacy needs and concerns of New Zealanders
- understand the Office's wide range of audiences and how to best reach them
- develop fit-for-purpose content for our audiences and deploy this through the most impactful channels.

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, prosecuting breaches, issuing compliance notices where necessary and monitoring 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. They produce Insights Reports 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 strategies and initiatives and will advise the Commissioner on the best way for the Office to achieve its mission. This team also leads the Office's work to engage and partner with Māori.

Appendix B

Information Matching 2020/21

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 section 184 the Commissioner recommends whether a provision should continue, be amended or be cancelled.

This year the Office issued four reports reviewing information matching provisions.

Department of Internal Affairs, Government Super Fund, Ministry of Education, Ministry of Health, National Provident Fund, and Waka Kotahi New Zealand Transport Agency information matching

This report covered provisions under section 78A and Schedule 1A of the Births, Deaths, Marriages, and Relationships Registration Act 1995. I recommended that the following provisions be repealed as they become replaced by AISAs:

- Disclosure of information to the Department of Internal Affairs
- Disclosure of life event information to the Government Superannuation Fund
- Disclosure of birth, name change, and death information to the Ministry of Education
- Disclosure of life event information to the National Provident Fund
- Disclosure of information to Waka Kotahi.

I also recommended that the provision for the disclosure of birth, name change, and death information to the Ministry of Health continue.

Ministry of Education and Teaching Council Teachers Registration information matching

This report covered matching under section 360 of the Education Act 1989. I recommended that the provisions continue, pending the re-evaluations of their use of the provision by both the Teaching Council and the Ministry of Education.

Electoral Act 1993, sections 263A and 263B

This report covered matching under sections 263A and 263B of the Electoral Act 1993 for the purpose of inviting eligible persons to enrol. I recommended that the provision continue, and supported the Electoral Commissioner's proposal that consideration be given to extending the contact information which may be provided under 263B.

Births, Deaths, Marriages, and Relationships Registration Act 1995, section 78A; Immigration Act 2009, section 300; Social Security Act 2018, schedule 6, clause 13

This report covered three provisions:

- Births, Deaths, Marriages, and Relationships Registration Act 1995, section 78A – which provides for death information to be provided to Inland Revenue
- Immigration Act 2009, section 300 – which provides for Immigration New Zealand information to be provided to the Ministry of Health for checking public funding eligibility
- Social Security Act 2018, schedule 6, clause 13 – which provides for Ministry of Social Development information to be provided to the Ministry of Justice for tracing fines defaulters.

The Commissioner considers that the authority conferred by these information matching provisions should be continued without amendment.

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

Changes in authorised and operating programmes

Currently operating:

There were 43 information matching programmes in operation, and seven programmes that were not active.

New provisions and programmes

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

The Ministry of Social Development (MSD) advise that they are exchanging information under existing social welfare reciprocity agreements with Canada, Denmark, Greece, Ireland, and the UK on behalf of Jersey and Guernsey. As there were no information exchanges reported under these agreements in previous years, we are working with MSD to clarify their reporting obligations under the Social Security Act 2018, section 384.

Programmes suspended

The Ministry of Business, Innovation and Employment did not operate their programme with Customs to identify people who might qualify as motor vehicle traders (Motor Vehicle Sales Act 2003, sections 120 and 121).

The Ministry of Education did not operate their programme with the Department of Internal Affairs (DIA) for birth records but are working on re-starting this programme and incorporating Name Change and Death information (Births, Deaths, Marriages and Relationship Registration Act 1995, section 78A).

The Ministry of Justice did not operate their programme with Immigration New Zealand for arrival and departure information to help locate people who owe fines because of the significant manual effort involved and the comparatively low benefits from the programme. The Ministry are considering alternative approaches to receive the information (Immigration Act 2009, section 295).

MSD also did not need to use the provision to allow Inland Revenue to respond to tax information enquires from the Netherlands social welfare authorities, as no requests were received from the Netherlands (Social Security Act 2018, section 385(3) and Tax Administration Act 1994, section 85B).

MSD did not use powers to require information for matching from employers under clauses 6 and 7 of Schedule 6 of the Social Security Act 2018 (was section 11A of the Social Security Act 1964).

MSD did not operate their Periods of Residence sampling match with Australia for superannuation entitlement. MSD advise that as Australia's concerns with Australian privacy law have been resolved they may resume operating the programme (Social Security Act 2018, section 380 and Social Welfare (Reciprocity with Australia) Order 2017).

Programmes ceasing

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




- Citizenship/DIA Passports
- BDM/DIA Passports
- BDM Births & Marriages/ Citizenship applications
- 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. There are three levels:

-  **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.




Accident Compensation Act 2001, section 246 and Tax Administration Act 1994, Schedule 7 Part C subpart 2 clause 41	Compliance
<p>1. IR/ACC Compensation and Levies</p> <p>To confirm income amounts for compensation calculations.</p> <p>Inland Revenue (IR) disclosure to ACC: For self-employed people, IR provides ACC with the full name, contact details, date of birth, IR number, and earnings information. For employers, IR provides ACC with the name, address, IR number, and total employee earnings.</p>	
	
Accident Compensation Act 2001, section 280	Compliance
<p>2. Corrections/ACC Prisoners</p> <p>To ensure that prisoners do not continue to receive earnings-related accident compensation payments.</p> <p>Corrections disclosure to ACC: Corrections provides ACC with the surname, given names, date of birth, gender, date received in prison, and any aliases of all people newly admitted to prison.</p>	
	
Accident Compensation Act 2001, section 281	Compliance
<p>3. ACC/MSD Benefit Eligibility</p> <p>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.</p> <p>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, section 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)/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>6. 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. 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 – CDs used for transfer not destroyed promptly.</p>	
<p>7. 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>8. 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>9. 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, gender, date and place of birth, date and place of death, and cause(s) of death.</p>	
<p>10. 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>Not compliant – minor technical issue – data not deleted promptly.</p>	

Births, Deaths, Marriages, and Relationships Registration Act 1995, section 78A (continued)	Compliance
<p>11. 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 Aotearoa New Zealand (if not born in Aotearoa New Zealand).</p>	
<p>12. 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: 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>13. 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>14. 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>15. 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>	

Citizenship Act 1977, section 26A	Compliance
<p>16. 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 Aotearoa 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>17. 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>18. 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, section 180	Compliance
<p>19. 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, section 181 and Immigration Act 2009, section 294	Compliance
<p>20. 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, section 306	Compliance
<p>21. Customs/IR Student Loan Alerts</p> <p>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.</p> <p>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.</p> <p>Customs disclosure to IR: Customs provides IR with the person's arrival card information. This includes the full name, date of birth, and date, time, and direction of travel including New Zealand port and prime overseas port (last port of call for arrivals and first port of call for departures).</p>	
<p>22. Customs/IR Student Loan Interest</p> <p>To detect student loan borrowers who leave for, or return from, overseas so that IR can administer the student loan scheme and its interest-free conditions.</p> <p>IR disclosure to Customs: IR provides Customs with the full name, date of birth, and IR number for student loan borrowers who have a loan of more than \$20.</p> <p>Customs disclosure to IR: For possible matches to borrowers, Customs provides the full name, date of birth, IR number and date, time and direction of travel.</p>	
Customs and Excise Act 2018, section 307	Compliance
<p>23. Customs/IR Child Support Alerts</p> <p>To identify parents in serious default of their child support liabilities who leave for or return from overseas so that IR can take steps to recover the outstanding debt.</p> <p>IR disclosure to Customs: IR provides Customs with the full name, date of birth, and IR number of parents in serious default of their child support liabilities.</p> <p>Customs disclosure to IR: Customs provides IR with the person's arrival card information. This includes the full name, date of birth, and date, time, and direction of travel including New Zealand port and prime overseas port (last port of call for arrivals and first port of call for departures).</p>	
Customs and Excise Act 2018, section 310	Compliance
<p>24. Customs/Justice Fines Defaulters Alerts</p> <p>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.</p> <p>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.</p> <p>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.</p>	
Education and Training Act 2020, schedule 3 clause 9	Compliance
<p>25. 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 clause 7	Compliance
<p>26. 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 clauses 8 & 9	Compliance
<p>27. 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, section 263A	Compliance
<p>28. 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>	

Electoral Act 1993, section 263B	Compliance
<p>29. DIA (Citizenship)/EC Unenrolled Voters</p> <p>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.</p> <p>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).</p>	
<p>30. DIA (Passports)/EC Unenrolled Voters</p> <p>To compare passport records with the electoral roll to:</p> <ul style="list-style-type: none"> • 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. <p>Passports (DIA) disclosure to Electoral Commission: Passports provides full name, date of birth, and residential address of passport holders aged 17 years and over.</p>	
<p>31. MSD/EC Unenrolled Voters</p> <p>To compare MSD's beneficiary and student databases with the electoral roll to:</p> <ul style="list-style-type: none"> • 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. <p>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 flagged as confidential.</p>	
<p>32. NZTA (Driver Licence)/EC Unenrolled Voters</p> <p>To compare the Driver Licence Register with the electoral roll to:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>	
<p>33. NZTA (Vehicle Registration)/EC Unenrolled Voters</p> <p>To compare the motor vehicle register with the electoral roll to:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>	

Electronic Identity Verification Act 2012, section 39	Compliance
<p>34. 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 still born 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, and 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>	
	
Motor Vehicle Sales Act 2003, sections 122 and 123	Compliance
<p>35. 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, section 380 and Social Welfare (Reciprocity with Australia) Order 2017	Compliance
<p>36. 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>	
	
Social Security Act 2018, section 380 and Social Welfare (Reciprocity with Malta) Order 2013	Compliance
<p>37. 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, section 380 and Social Welfare (Reciprocity with the Netherlands) Order 2003	Compliance
<p>38. Netherlands/MSD Change in Circumstances</p> <p>To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and the Netherlands.</p> <p>MSD disclosure to Netherlands: MSD forwards the appropriate application forms to the Netherlands Sociale Verzekeringsbank (SVB). The forms include details such as the full names, dates of birth, addresses, and MSD client number.</p> <p>Netherlands disclosure to MSD: SVB responds with the SVB reference number.</p>	
<p>39. Netherlands/MSD General Adjustment</p> <p>To enable the processing of general adjustments to benefit rates for individuals receiving pensions from both New Zealand and the Netherlands.</p> <p>MSD disclosure to Netherlands: For MSD clients in receipt of both New Zealand and Netherlands pensions, MSD provides the Netherlands Sociale Verzekeringsbank (SVB) with the changed superannuation payment information, the MSD client reference number, and the Netherlands unique identifier.</p> <p>Netherlands disclosure to MSD: SVB advises adjustments to payment rates and the 'holiday pay' bonus.</p>	
Social Security Act 2018, section 380 and Social Security (Reciprocity with the United Kingdom) Order 1990	Compliance
<p>40. United Kingdom/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 United Kingdom.</p> <p>UK disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information, and Social Security numbers.</p> <p>MSD disclosure to UK: Includes full name, date of birth, marital status, address, entitlement information, and New Zealand Client Number.</p>	
Social Security Act 2018, Schedule 6, clause 13	Compliance
<p>41. MSD/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 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.</p> <p>MSD disclosure to Justice: For matched records, MSD returns the last known residential address, postal address, residential, cell-phone and work phone numbers, and the unique identifier originally provided by Justice.</p>	
Social Security Act 2018, Schedule 6, clause 15	Compliance
<p>42. 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>	
Tax Administration Act 1994, section 85A (replaced by Schedule 7 Part C subpart 2 clause 43)	Compliance
<p>43. 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>	

Appendix C

Independent Auditor's Report

To the readers of the Privacy Commissioner's financial statements and performance information for the year ended 30 June 2021

The Auditor-General is the auditor of the Privacy Commissioner. The Auditor-General has appointed me, Lauren Clark, using the staff and resources of Audit New Zealand, 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 44 to 61, that comprise the statement of financial position as at 30 June 2021, 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 10 to 20 and pages 30 to 43.

In our opinion:

- the financial statements of the Privacy Commissioner on pages 44-61:
 - present fairly, in all material respects:
 - its financial position as at 30 June 2021; 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 10 to 20 and pages 30 to 43:
 - presents fairly, in all material respects, the Privacy Commissioner's performance for the year ended 30 June 2021, 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 appropriation; and
 - the actual expenses or capital expenditure incurred compared with the appropriated or forecast expenses or capital expenditure and
 - complies with generally accepted accounting practice in New Zealand.

Our audit was completed on 20 December 2021. This is the date at which our opinion is expressed.

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 is responsible for the other information. The other information comprises the information included on pages 2 to 9, 21 to 29, and 62 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.



Lauren Clark
Audit New Zealand

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

© 2021 The Privacy Commissioner
ISSN 1179-9838 (Print)
ISSN 1179-9846 (Online)