

PRIVACY COMMISSIONER

Annual Report 2020



Annual Report of the Privacy Commissioner

for the year ended 30 June 2020

Presented to the House of Representatives pursuant to section 24 of the Privacy Act 1993

The Minister of Justice

I tender my report as Privacy Commissioner for the year ended 30 June 2020

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

John Edwards
Privacy Commissioner
December 2020

Introduction	1
Key points	3
Timeline	5
Working towards our strategic goals	7
Report on activities	9
Law reform	10
Dispute resolution	11
Codes of practice	16
Policy	17
Outreach	20
International	22
Enquiries and education	24
Breach notifications	25
Information matching	27
Office and functions	29
Independence and competing interests	30
Reporting	30
Staff	31
Covid-19	31
EEO profile	32
Finance and performance report	33
Statement of responsibility	34
Statement of performance	35
Statement specifying comprehensive income	36
Cost of service statement for the year ended 30 June 2020	37
Output class 1: Guidance, education and awareness	39
Output class 2: Policy and research	41
Output class 3: Information sharing and matching	43
Output class 4: Compliance	44
Statement of accounting policies for the year ended 30 June 2020	45
Statement of comprehensive revenue and expenses for the year ended 30 June 2020	47
Statement in changes of equity for the year ended 30 June 2020	48
Statement of financial position as at 30 June 2020	49
Statement of cash flows for the year ended 30 June 2020	50
Notes to the financial statements for the year ended 30 June 2020	51
Appendices	67
Appendix A – Processes and services	68
Appendix B – Information matching programme compliance	69
Appendix C – Auditor’s Report	81

Introduction

Privacy Act 2020 becomes law

The Privacy Bill was introduced to Parliament in March 2018. On 30 June 2020, the Bill received the Royal Assent. It came into effect on 1 December 2020. The new Act significantly updates the 1993 Act. Many of the changes to the law are based on recommendations from the Law Commission's comprehensive 2011 review of New Zealand's privacy laws.

Key changes in the new law include:

- new criminal offences
- introduction of compliance orders
- binding access determinations
- controls on the disclosure of information overseas
- mandatory notification of harmful privacy breaches
- the law now explicitly applies to overseas-based entities that carry on business in New Zealand.

Privacy 2.0

The new Privacy Act gives the Privacy Commissioner a range of new enforcement tools. We took the opportunity implementing the new Act provided to examine our approaches and rethink our priorities. We called this internal reassessment process, Privacy 2.0.

Privacy 2.0 made us think hard about how best to apply our resources to maximise our impact for New Zealanders. We considered our existing functions, examined potential new functions and looked at how we will assess and prioritise future incoming work.

Following this review, we agreed upon some key changes:

- To establish a Compliance and Enforcement team responsible for identifying, assessing and acting on systemic issues that meet our enforcement priorities.
- To establish a Strategy and Insights function to: help proactively develop a Te Ao Māori and privacy strategy; understand existing and emerging trends and technological developments that are relevant to the OPC's mission; and monitor the success of our strategies and initiatives.
- To create new roles to support the strategic direction, including a new Assistant Commissioner (Strategy and Insights) and a Principal Advisor Māori.

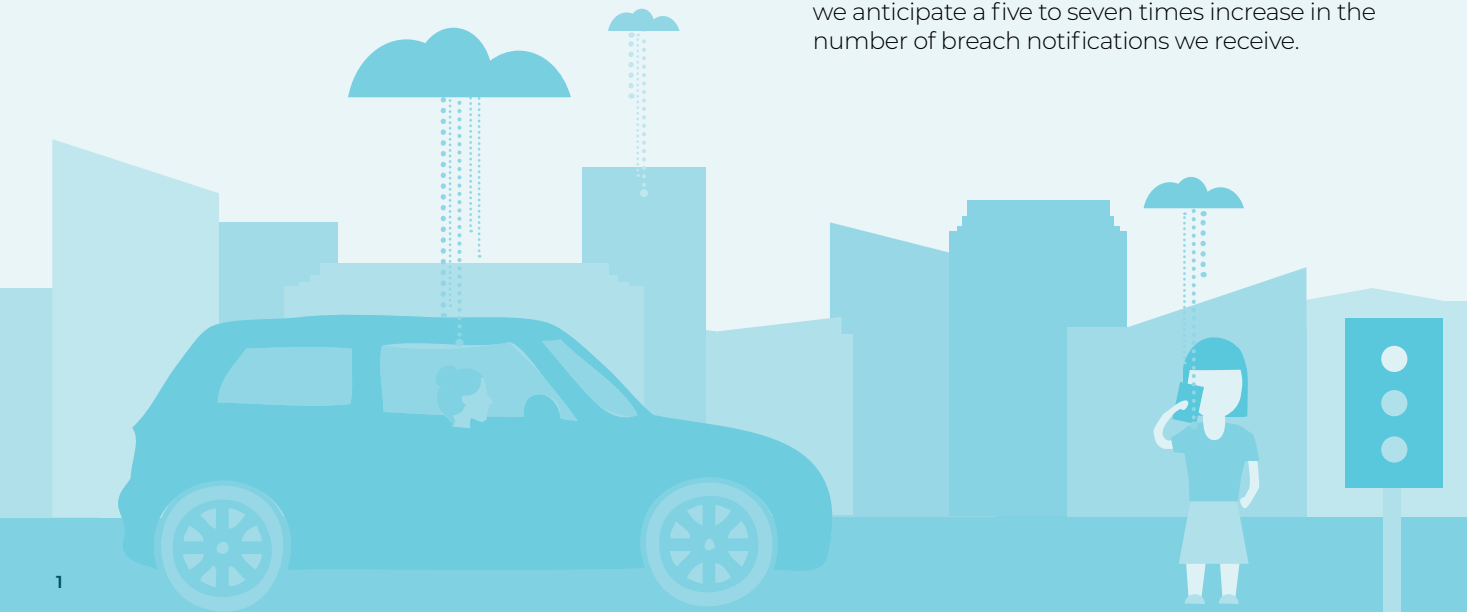
Development of privacy breach reporting tool, NotifyUs

Throughout the reporting period, we worked with organisations in the public and private sectors to develop a tool ("NotifyUs") that would enable organisations to easily meet their statutory obligations to report their privacy breaches to us.

Under the Privacy Act 1993, it was voluntary for organisations to report privacy breaches to us. Under the Privacy Act 2020, organisations have an obligation to report serious privacy breaches to the Privacy Commissioner and, in most cases, to affected parties. Failure to do this could result in the organisation receiving fines of up to \$10,000.

NotifyUs will help organisations determine whether their breach must be reported, and will guide people through the reporting process.

Based on experience from countries we compare ourselves to that have implemented similar regimes, we anticipate a five to seven times increase in the number of breach notifications we receive.



Covid-19

In the first half of 2020, Covid-19 rapidly upended societal norms as countries across the globe enacted stringent lockdowns to combat the pandemic.

New Zealand's 'Unite Against Covid-19' response included measures such as contact tracing registers, limits on free movement and stay at home orders. From February onwards, we advised on and assessed the privacy impacts of policies and solutions that the Government and private businesses were rolling out to tackle Covid-19.

We produced a stocktake of contact tracing apps, including the Ministry of Health's app, and assessed each solution's privacy compliance. We dealt with numerous media enquiries and awarded a Privacy Trust Mark to Rippl's contact tracing app, recognising its clear communication to users about how personal information was handled.

We also participated in a Global Privacy Assembly hosted COVID-19 Taskforce, which was formed to drive practical responses to privacy issues emerging from the pandemic

Despite closing our premises during the lockdown periods, the pandemic and lockdown measures appear to have had little effect on our ability to deliver services in accordance with our standard key performance indicators.

International privacy developments

Due in part to the new stronger rules under California's Consumer Privacy Act and Europe's General Data Protection Regulation (GDPR), some tech companies have started to implement internal reforms. Multiple tech platforms are now shifting their business model from users having to "opt out" of default intrusive data-gathering practices to giving them the option to "opt in".

In June 2020, Google changed its default data practice so that new users of their services will have their personal data automatically deleted after 18 months.

EU adequacy review

Data adequacy status is granted by the European Commission to countries outside of Europe which have a level of privacy protection comparable to that under European law. New Zealand was recognised with "adequacy" status in 2012, and throughout the reporting period the European Commission has been undertaking a periodic review of that status. We provided ongoing assistance to Ministry of Justice and MFAT officials regarding the current review. We met with European Commission officials via video conference and provided advice and responses to questions raised in the review about the operation of New Zealand's privacy laws.



Key points

Law reform

- The Privacy Bill received the Royal Assent on 30 June 2020.
- Throughout the year, we worked closely with the Ministry of Justice and others in preparation for the new law.

Dispute resolution

- We closed 769 investigation files.
- At the end of the reporting year, 89% of open investigation files were less than six months old.
- The total value of settlements from investigations closed by OPC in 2019/20 was \$216,400.
- An external audit of our investigations for the reporting year gave 95% a score of 3.5 or higher out of 5.
- We referred three cases to the Director of Human Rights Proceedings.
- Twenty-three complainants took proceedings to the Tribunal themselves.
- No agencies were named for non-compliance with the Privacy Act under our naming policy.

Codes of practice

- We amended the Telecommunications Information Privacy Code, extending the emergency caller location system.
- We also amended the Civil Defence National Emergencies (Information Sharing) Code during the March Covid-19 lockdown.

Policy

- We advised on 133 policy proposals that involved personal information and published 14 submissions.
- Our team received an award from the Global Privacy Assembly for our 2019 inquiry into the Ministry of Social Development's misuse of its fraud investigation powers.

Outreach

- We gave 89 in-person presentations to a diverse range of groups.
- We commissioned our bi-annual privacy attitudes survey of 1,398 New Zealanders.
- We produced a series of podcasts educating people about the new Privacy Act.
- We awarded grants to four projects through our Privacy Good Research Fund.

International

- Many international events the Office would normally attend were moved online due to Covid-19.
- We provided assistance to Ministry of Justice officials regarding review of New Zealand's EU adequacy status.
- In late 2019, we participated in the Global Privacy Assembly (GPA) in Tirana, Albania, and the Asia Pacific Privacy Authorities (APPA) Forum in the Philippines.
- We regularly take part in Global Privacy Enforcement Network teleconferences.
- During May and June we, along with the GPA, OECD and APPA, participated in the Global Privacy Assembly's COVID-19 Taskforce meetings. These meetings were tasked with driving practical responses to privacy issues emerging from the pandemic.



Enquiries and education

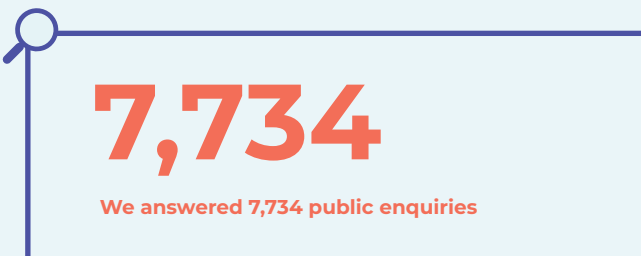
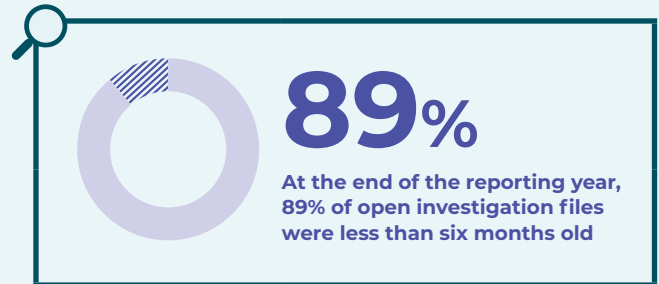
- We answered 7,734 public enquiries.
- 12,725 people completed one of our e-learning modules during the reporting year.
- We responded to 291 media enquiries.
- We awarded two Privacy Trust Marks, recognising excellence in privacy.

Breach notifications

- Agencies reported 205 privacy breaches to us. This number is expected to substantially increase under the new Privacy Act.
- We worked with multiple organisations in the public and private sector to develop NotifyUs, a new breach reporting tool. The tool will make it easy for organisations to report privacy breaches to us.
- We developed new guidance to help organisations and individuals understand how to prevent and respond to privacy breaches.

Information matching

- There were 47 information matching programmes in operation and six inactive programmes this reporting year.
- We issued three reports reviewing 15 information matching provisions.
- Four information matching programmes are still being transferred to operating under Approved Information Sharing Agreements (AISAs). DIA is also working towards transferring additional programmes from information matching provisions to AISAs.



Timeline

1 July 2019

First day of reporting year

7 August 2019

Privacy Bill passes second reading in Parliament

16 October 2019

Privacy Commissioner intervenes in the Taylor proceedings in the High Court

24 October 2019

The Office of the Privacy Commissioner wins an international award for its inquiry and report into MSD's misuse of its fraud investigation powers

December 2019

OPC works with NZ Police on firearm buy-back privacy breach

October 2019

Privacy Commissioner launches illion inquiry

September 2019

Cross-office team begins work on new privacy breach reporting tool

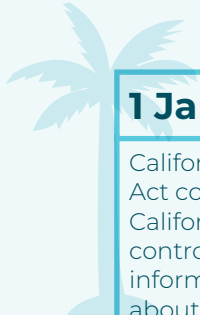
December 2019

Privacy Good Research Fund recipients announced

20 December 2019

Privacy Commissioner launches inquiry into Trade Me's update to its privacy policy





1 January 2020

California Consumer Privacy Act comes into force giving Californian consumers more control over the personal information companies collect about them.



April-May 2020

OPC works with MoH and others on privacy considerations regarding contact tracing registers and NZ Covid Tracer app

3 June 2020

Privacy Bill moves to Committee of the Whole House

30 June 2020

UMR public attitude survey results released

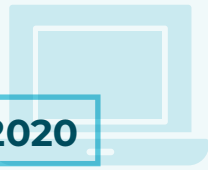
24 June 2020

- Privacy Bill passes third reading in Parliament
- Trust Integrity Compliance's anti-money laundering platform and the Rippl contact-tracing app are awarded fourth and fifth Privacy Trust Marks



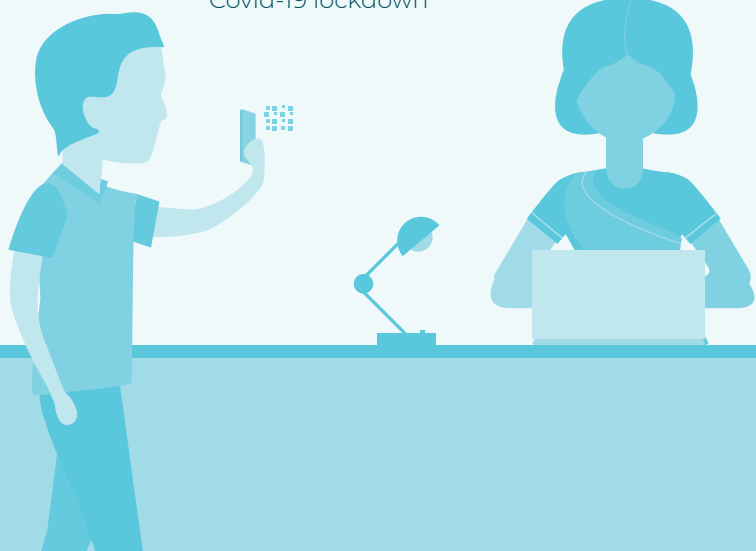
25 March 2020

All OPC staff begin to work remotely due to Covid-19 lockdown



30 June 2020

Privacy Act receives the Royal Assent, with the new Act to take effect on 1 December 2020



Working towards our strategic goals

We aim to make privacy accessible and understandable for all New Zealanders. By educating the public about the Privacy Act and their rights and obligations under it, our goal is for New Zealanders to benefit from safe and responsible personal information practices.

In our Statement of Intent 2017-2021, we identified three outcomes:

Outcome 1 Increased citizen and consumer trust in the digital economy



Businesses and government benefit from the use of people's personal information. New technologies have increased the value of that information and make it easier to access than ever before.

New Zealand needs citizens and consumers to trust agencies with their personal information. By providing effective regulation and promoting good privacy practices, we play a key role in building that trust.

Progress made

Over the past year, the Commissioner and Office promoted citizen and consumer trust in the digital economy by regularly engaging with media, writing blogs and articles, producing podcasts and answering the public's questions through our website's FAQ service. We regularly receive positive feedback from our stakeholders, primarily through public engagement on our main social media channels (Twitter, LinkedIn and Facebook).

In April 2020, we conducted our biannual UMR privacy attitudes survey. Of those surveyed, 56 percent reported being concerned about individual privacy and the protection of personal information, down 11% on 2018. Overall, respondents were most concerned about businesses sharing personal information without their permission (75%, down 4%). The survey's margin of error was +/- 3.1%.

During lockdown, the Commissioner made numerous media appearances discussing concerns about the privacy implications of government mandated contact tracing measures.

In June, we published a stocktake of contact tracing solutions available in the New Zealand market, providing information about how each collected and handled users' personal information. We assured the public that using the Ministry of Health's contact tracing app was safe and secure and answered dozens of public queries about contact tracing and other Covid-related privacy issues.

Our Investigations and Dispute Resolution team provided independent and effective dispute resolution services via phone and online for individuals with privacy complaints.

Outcome 2 Innovation is promoted and supported



Privacy is no impediment to technological advancement. We want to work across the public and private sectors to encourage innovation while keeping personal information safe.

Progress made

Last reporting year, we received a grant from the International Association of Privacy Professionals ANZ Legacy Fund. This grant, and financial support from the Social Investment Agency (SIA), enabled us to run a second round of the Privacy Good Research Fund. We sponsored four diverse and innovative privacy research projects. The projects were due to be completed in late 2020.

The new Privacy Act will require all agencies to notify us if they experience a serious privacy breach. To make reporting as simple as possible, we developed a tool called NotifyUs that enables organisations to report potentially serious privacy breaches to us. As part of this process, we consulted extensively with external agencies in the private and government sectors to ascertain their requirements for a breach notification tool, and to make NotifyUs useful and user-friendly. The tool went live on our website in October 2020.

Our Privacy Trust Mark scheme, which recognises excellence in privacy-friendly products or services, awarded two additional Trust Marks this reporting year, bringing the total to six. The scheme encourages organisations to consider privacy as they innovate and advance their practices.

We released several new e-learning modules including Privacy ABC for Schools and Privacy 2020, an overview of the new Privacy Act. We now have 11 modules covering a diverse range of issues affecting privacy, with around 1,200 people a month completing at least one of our courses.

Outcome 3 Increased influence to improve personal information practices



Building relationships with agencies is the most effective way we can help improve their personal information practices.

Progress made

Throughout this period, we continued to strengthen our connections with key stakeholders.

In May, we worked with the Ministry of Health on the rollout of their NZ Covid Tracer app, ensuring it adhered to privacy principles. Following the app's release, the Commissioner made public statements assuring New Zealanders that the app protected and respected their privacy.

In early 2020, we joined with the likes of Police, Netsafe, DIA and other agencies as part of the Internet Trust and Safety Alliance. This group meets to discuss pertinent cross-government issues and share information and updates about the projects each organisation is working on.

We also hosted secondees from Waka Kotahi NZ Transport Agency and ACC, who worked with us for six-monthly stints in our Investigations team. Bringing in expertise from other agencies helps us and the other organisations learn from each other. Secondees can then take valuable privacy knowledge back to their home organisation to improve their practices. One of our senior staff members was seconded to the Office of the Australian Information Commissioner to assist their dispute resolution programme.

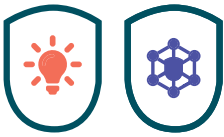
We continued to develop our relationships with stakeholders such as CERT NZ, Consumer NZ, Internet NZ, regional law societies, the Institute of Directors and various district health boards through our regional visits, public presentations and consultations on key projects.

Look for activities marked with these icons to find out what else we have been doing to fulfil our outcomes



Report on activities



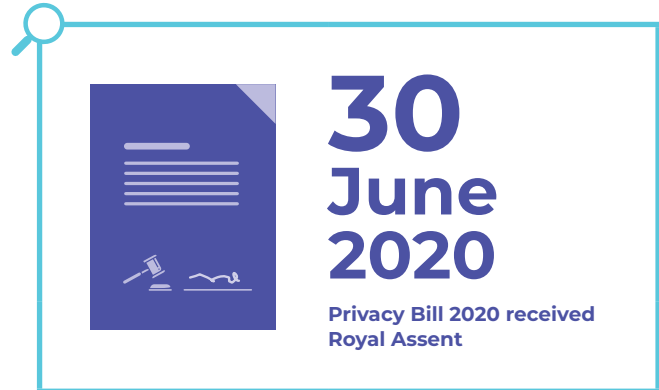


Law reform

The Privacy Bill had its third reading during an urgent sitting of Parliament on 24 June 2020. It passed with unanimous support and received Royal Assent on 30 June 2020. The Privacy Act 2020 came into force on 1 December 2020.

Leading up to enactment, we continued to work closely with Ministry of Justice officials to provide advice on Supplementary Order Paper 482, addressing minor policy matters and necessary clarifications.

Amendments included: clarification of the application of the Bill; liability for failing to notify the Privacy Commissioner of a privacy breach; and ensuring that complaints and proceedings in the Tribunal can be brought by a representative of a class of individuals. The Supplementary Order Paper was released on 17 March 2020 and was adopted unanimously during the Committee of the Whole House on 3 June 2020.





Dispute 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. The team works with a diverse range of complainants and respondents to resolve all manner of complex privacy issues. Some investigations result in compensation or other remedies for complainants.

This reporting year we closed 769 investigation files, a 14% decrease on 2018/19. Seventy-nine (79%) of these files were closed within six months. As at 30 June 2020, 89% of the open investigation files were less than 6 months old, which fell slightly short of meeting our KPI of 90%.

We regularly employ external auditors to conduct reviews of our investigations. Files reviewed by the auditor for the period 1 July 2019 – 30 June 2020 received an average score of 4.07 out of 5. Ninety-five percent (95%) of our investigators' files scored 3.5 or higher.

Figure 1
Age of open complaint files as at 30 June 2020

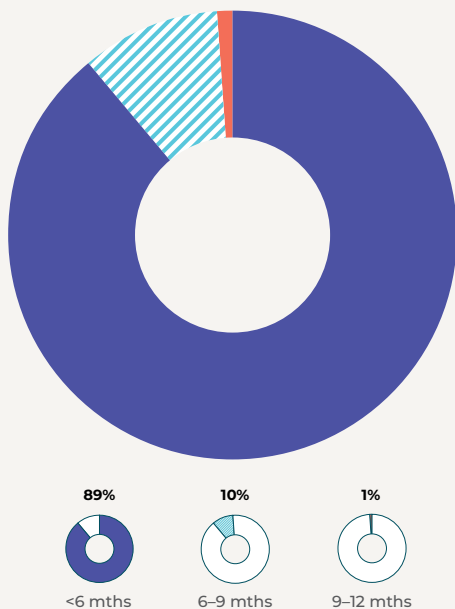
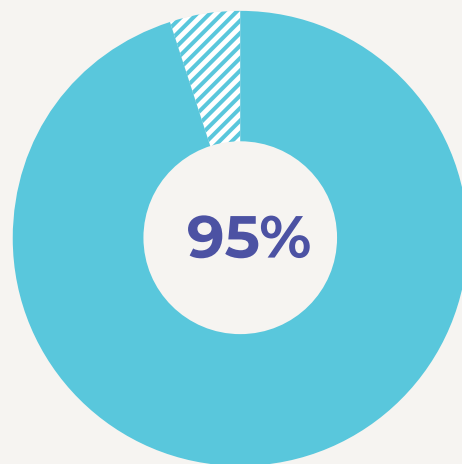


Figure 2
Result of complaint file reviews



95% of investigations assessed by an independent reviewer received a score of 3.5 or higher

Case examples

CASE ONE

Power company discloses man's address to estranged ex-partner

A farmer advised his power company that he was shifting to a new farm in order to avoid his ex-partner. The man's former partner had a history of violent threats and harassment against him and had been issued a trespass notice, which she had repeatedly breached.

He asked the company to send his bills to a new email address, which his ex-partner did not have access to. Soon after, the company mistakenly sent a bill containing his new physical address details to his old email. The man's ex-partner saw his address and a short time later began driving by his new property and leaving threatening letters in his mailbox.

The power company apologised to the man, blaming both human and system error. They offered him a compensation package worth approximately \$10,000. The man felt this was insufficient for the harm he had suffered and contacted our office.

The man's complaints raised issues under principles 5, 8 and 11 of the Privacy Act. Principle 5 obliges organisations to ensure personal information they hold is protected by reasonable security safeguards to secure against loss, access, use, modification, disclosure or misuse. Principle 8 provides organisations should not use personal information without taking reasonable steps to ensure it is accurate, up to date, complete, relevant and not misleading. Principle 11 sets out that agencies shall not disclose personal information they hold unless they believe, on reasonable grounds, that one of the exceptions listed in principle 11 applies.

We contacted the power company which admitted breaching the man's privacy. They argued they did have adequate safeguards to protect customers' data in place, but stated that no system is completely fail safe.

They explained the circumstances that had led to the breach occurring and offered to make a slight increase to their offer of compensation. We put the offer to the complainant, who rejected it.

We facilitated a teleconference to try to reach a settlement that was satisfactory for both parties. The farmer explained that after his ex-partner had found out his new address, he had to uproot and move to a new farm, at significant personal expense. He wished to be reimbursed for those costs and compensated for the emotional harm the incident had caused him and his new partner.

After further negotiations facilitated by us, the power company agreed to pay the man \$24,000 in addition to the \$10,000 package that was initially offered.

A settlement was drawn up to which both parties agreed. The farmer was paid, and no further action was taken.

CASE TWO

Charity shop failed to notify CCTV cameras recorded audio

A charity shop volunteer complained to our office after discovering CCTV cameras in the shop they worked for were recording audio without the knowledge of customers or other staff.

While there was signage in the store advising that CCTV was in operation, the sign did not warn that there was audio recording. The volunteer felt uncomfortable that their conversations in the shop were being recorded. They also suspected that there might be audio recording in the break room. They spoke with the manager and contacted head office with their concerns but felt unhappy with the response. This led the volunteer to resign from their position at the shop and contact the Privacy Commissioner to complain.

This complaint raised issues under principles 1, 3 and 4 of the Privacy Act. Under principle 1, an agency must not collect personal information unless it is for a lawful purpose connected with a function or activity of the agency, and collection is necessary for that purpose. Under principle 3, when an agency collects personal information, it shall take reasonable steps to ensure the individual concerned is aware of what is being collected. Under principle 4, an agency must not collect information in an unlawful or unfair way, or in a way which intrudes to an unreasonable extent upon the personal affairs of the individual involved.

We contacted the charity shop and communicated the complainant's concerns and the Commissioner's view that audio recording throughout the store was unreasonably intrusive. We asked for the shop's management to advise of the location of each of their surveillance cameras and the purpose for collecting this information.

We also asked the charity shop to advise the public and its employees that audio surveillance was taking place. We recommended they have a robust policy around storage and retention, and that audio recordings not be kept for longer than necessary. We said that as the cameras capture personal information, members of the public, staff and volunteers had the right to access that information under principle 6.

Finally, we recommended the shop issue an apology to the complainant for the distress caused.

The store's management told us that audio recording assisted with customer complaints, stating that it provided additional information and context to the video stream. This helped them with "retrospective analysis of any incident".

In response to our recommendations, the charity shop advised us that they had permanently disabled the audio capability in four of their six in-store cameras except for those at point of sale and one other area. They confirmed that no recording, audio or otherwise, was taking place in the break room. They said they had strengthened guidance for public and staff for any audio captured from the system and had committed to upgrading signage which would state "this camera records audio".

We gave the complainant a Certificate of Investigation and advised them of their right to take the complaint to the Human Rights Review Tribunal should they wish. We then closed the complaint.

Organisation withholds information to protect manager's privacy

A woman requested a copy of a draft report from her former employer who had investigated her former manager's alleged bullying.

The employer gave her the draft report but withheld information to protect the privacy of other individuals, including the manager.

The woman wished to see the full, unredacted draft report and made a complaint to us.

The woman's complaint raised issues under principle 6 of the Privacy Act. Under principle 6, individuals have a right to request access to personal information held by an organisation, subject to the withholding grounds in Part 4 of the Act.

When a person requests information about themselves that is mixed with that of other people, it can be difficult for agencies to balance someone's right to access information about themselves against other people's right to privacy. Agencies must therefore consider the following:

1. If the information is about the requester.
2. If the information includes information about other people.
3. If the disclosure of other people's information would be unwarranted.

We contacted the organisation, who responded with concerns about releasing the content of the draft report to the former employee. It said:

- The report included interviews with other former staff members who could not consent to the release of the information.
- Some staff had spoken in confidence due to concerns their comments would be seen by the manager accused of bullying. The employer said it was necessary to withhold the names of those staff to protect their identities and maintain confidentiality.
- The former employer concluded the draft report was biased and inaccurate, and had decided not to proceed to a final report. It did not circulate the draft report on the basis that it could have exacerbated a tense working environment at the time.

After being notified of the complaint, the former employer reviewed the redactions and concluded that some were incorrectly made. However, it stood by its original decision to withhold some information under section 29(1)(a) of the Privacy Act.

Section 29(1)(a) enables agencies to withhold information from a requester if they are satisfied that such a disclosure would involve 'unwarranted' disclosure of the affairs of another person in the circumstances.

We decided that most of the draft report's content was about the complainant, but that it did include personal information about other individuals. The former employer had discussed the Terms of Reference of the complaint with the complainant and said that she would have an opportunity to see the report after any privacy concerns had been addressed. It appeared both the complainant and the manager were aware this was the process the former employer intended to follow.

Our view was that all personal information about the complainant in the draft report should be released and that the organisation did not have a proper basis for its decision to rely on section 29(1)(a) to refuse the request. Any information in the report that was not about the complainant was outside the scope of our investigation and could be withheld.

The former employer arranged for the complainant to view the report at her convenience, provided she did not take any photos or notes of its content. Given that the report contained mixed information about a few individuals, providing access to the report in this way balanced her right to access the information with the rights of the other individuals to have their information protected. The complainant accepted this condition and we closed the file.

When a person requests information about themselves that is mixed with that of other people, it can be difficult for agencies to balance someone's right to access information about themselves against other people's right to privacy.

CASE FOUR

Parents complain school mishandled their child's sensitive medical information

Two parents complained to us after a primary school displayed their child's Medical Action Plan (MAP) in the school staffroom.

MAPs are developed by schools to inform staff how to respond to children who may require urgent medical attention. The child had high needs and the MAP included sensitive medical information regarding their toileting.

The parents were informed the school would display the MAP in the school's staff room after their child brought home an unsealed letter and copy of the MAP they had been given.

The parents were concerned with the way the school delivered the information, which they believed should have been enclosed in an envelope or marked as confidential. They were additionally concerned with the placement of the MAP in the school's staffroom. They said pupils regularly entered the staffroom and could have easily viewed the MAP, which they said would have caused their child to be bullied and her dignity compromised. The parents complained to the school and the board of trustees.

The school responded that they did not believe they had breached the child's privacy but removed the MAP from the staffroom and subsequently reviewed the way children's medical information was accessed and shared by staff. The school later expressed regret to the parents.

The parents were not satisfied with the way the investigation was conducted and lodged a complaint with us. This complaint raised issues under principles 5 and 11 of the Privacy Act 1993.

Principle 5 says that agencies should take reasonable steps to ensure that personal information they hold is protected by security safeguards that are reasonable in the circumstances to protect against loss, unauthorised access or use. Principle 11 places limits on disclosures of personal information.

The school did not believe it had inappropriately displayed the child's MAP. They argued that not having this information easily accessible could compromise the school's ability to deal with students with serious health needs. They further argued that the staffroom was a private location, not open to students, and the most sensitive information in the document was known to other students, who were extremely kind to the child and sensitive to their problems.

Our investigation concluded that the school had breached principle 5 of the Privacy Act. Given the extremely sensitive nature of the child's medical condition, we did not believe the staffroom was the appropriate location to display the MAP. Although the staffroom was predominantly accessed by school staff, it was reasonable to assume that children or other adults may enter it.

We acknowledged the importance of having that information available to staff responsible for the child's health and safety, but that it was still important to ensure the information was only available to those with a need to know. The display in the staff room meant the information was subject to wider distribution than was necessary.

We recommended the school apologise to the parents and undertake privacy training. As the school removed the MAP from the staffroom and undertook steps to review its processes, we did not think further action from our Office was necessary.

Compliance Advice Letters

We introduced Compliance Advice Letters several years ago as an early resolution option designed to deal with complaints that may not meet the threshold to conduct a full investigation.

Compliance Advice Letters address a complainant's privacy issues and remind agencies of their Privacy Act obligations.

Below is an example of a complaint we addressed using a compliance advice letter.

EXAMPLE ONE

Shop asked to remove photos of innocent alleged shoplifter

A woman complained to us after CCTV footage and photos labelling her a shoplifter were posted to a Facebook group and on a storefront window. The woman had been arrested at the store for shoplifting, but Police later dropped the charges due to lack of evidence.

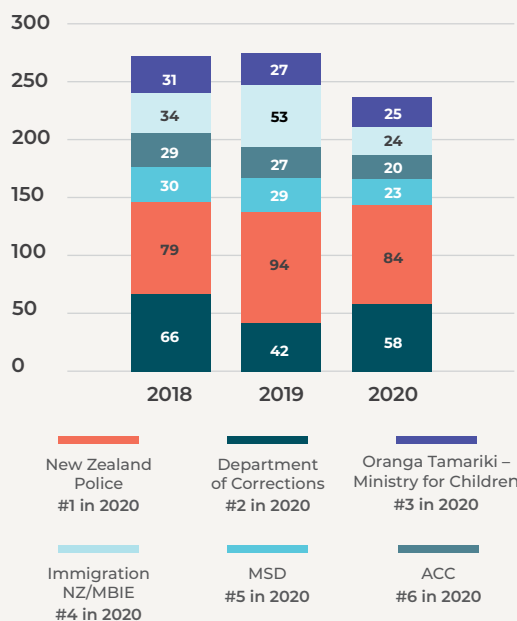
Identifying images of people are personal information. Our investigators sent a compliance advice letter to the shop stating the relevant privacy principles and explaining that publishing and sharing images without checking their accuracy could cause a person serious embarrassment.

The compliance advice letter also explained that while CCTV cameras could legitimately be used to detect and record crime, publication of photos and footage on social media meant to shame people was inconsistent with collecting personal information for security reasons.

The store removed the CCTV footage and the images of the woman from the storefront. No further action was taken.



Figure 3
Top complaints by agency



Human Rights Review Tribunal

Our goal is to resolve most complaints we receive during the course of the investigation. When parties are unable to reach an agreement, we can refer the matter to the Director of Human Rights Proceedings. The Director may then choose to take the case to the Human Rights Review Tribunal. Complainants also have the right to take their case to the Tribunal themselves.

Cases referred to the Tribunal

This reporting year we referred three cases to the Director (one referral related to two complaints).

Twenty-three complainants took proceedings to the Tribunal themselves without a referral from us. This was the same number as the previous year.

Tribunal decisions

We monitor Tribunal decisions with interest. They provide us with guidance in interpreting the law and forming views when investigating Privacy Act complaints.

The Tribunal issued 20 Privacy Act decisions this year. Of those, five decisions found an interference with privacy and three awarded damages to the plaintiffs. One decision (*Mills v Capital and Coast District Health Board* [2019] NZHRRT 47) awarded combined damages of \$40,000 (\$20,000 per defendant).

Another (*Vivash v Accident Compensation Corporation* [2020] NZHRRT 16) awarded \$45,000 with a further \$5,000 awarded as a contribution towards a plaintiff seeking legal advice on his entitlement to backdated weekly compensation of his 1985 claim.

In the third, the plaintiff was awarded \$3,000 (*Director of Human Rights Proceedings v Katui Early Childhood Learning Centre Ltd* [2019] NZHRRT 55).

Naming

We operate a naming policy in line with section 116(2) of the Privacy Act. Under the policy an agency may be formally named by the Privacy Commissioner where, on balance, he considers that the agency ought to be named for the purpose of giving effect to the Privacy Act.

In the 2019/20 year, no agencies were named under this policy (there was one in the previous year).



\$216,400

Total amount paid in settlements through the Dispute Resolution Process in 2019/20

Codes of practice

Six privacy codes of practice have been issued by the Privacy Commissioner. During the year the Civil Defence National Emergencies (Information Sharing) Code came into effect due to the declared state of national emergency and we amended the Telecommunications Information Privacy Code.

Civil Defence National Emergencies (Information Sharing) Code

On 25 March 2020, the Minister of Civil Defence, Peeni Henare, declared a state of national emergency under the Civil Defence Emergency Act 2020 in response to the Covid-19 pandemic. A declaration of a state of national emergency triggers the operation of the Civil Defence National Emergencies (Information Sharing) Code under the Privacy Act.

A declaration of a state of national emergency triggers the operation of the Civil Defence National Emergencies Code under the Privacy Act.

The activation of the Code permitted agencies to collect, use or disclose (to certain agencies) personal information for purposes directly related to the Government's management of the response to, and recovery from, the state of national emergency caused by the Covid-19 pandemic.

The Code ensured information could flow as required, helping agencies to respond quickly to the threat posed by Covid-19. The Code provides additional grounds to collect, use or disclose personal information that can be used alongside any other exception in the information privacy principles or code of practice, or any other legislative authority.

The Code was deactivated 20 working days after expiry of the state of national emergency on 11 June 2020.

TIPC amendment for Emergency Location Information System

The Privacy Commissioner issued Amendment No 7 to the Telecommunications Information Privacy Code 2003 on 8 April 2020, and it came into force on 7 May 2020.

The amendment extends the emergency caller location system contained in Schedule 4 of the Telecommunications Information Privacy Code. The system was first permitted by Amendment No 5 to the Telecommunications Information Privacy Code 2003.

It facilitates the active collection of location information from devices where necessary to prevent or lessen a serious threat to the life or health of an individual. The system still requires the existence of an emergency, but is no longer contingent on the making of an emergency call. The Emergency Caller Location Information System is now known as the Emergency Location Information System.

The amendment added privacy and accountability safeguards, including: access and use limitations; mandatory reporting of a disclosure log to the Commissioner; and a mandatory review of the operation of the system by the Privacy Commissioner, on or before 1 May 2022.

The amendment also requires after-the-fact notification of the use of the system to the individual concerned, where the emergency service providers collect location information in the absence of an emergency call. This serves as an important safeguard to allow affected individuals to challenge collections of location information in the absence of an emergency call that they believe to be unnecessary or unlawful.

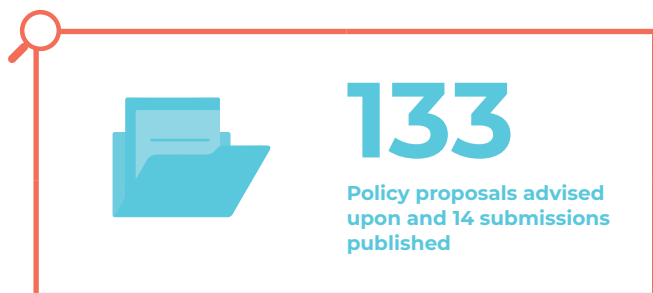
The Ministry of Business, Innovation and Employment is currently the relevant government agency for the purposes of Schedule 4 and is progressing work to implement the new functionality.

Policy

In an external audit of our policy files from the last year, 89% met or exceeded our quality standard of 3.5 out of 5. This year we advised on 133 policy proposals. We also published 14 submissions and 4 office research projects.

Credit Reporting Privacy Code – illion inquiry

In October 2019, we launched an inquiry into illion New Zealand and its related company Credit Simple (NZ) Ltd. The inquiry investigated whether they were complying with the Credit Reporting Privacy Code 2004, particularly the prohibitions on marketing by credit reporters and any of their related companies (e.g. companies that sit under the same corporate umbrella). The investigation concluded and the findings were released outside the reporting year.



Trade Me inquiry

In December 2019, we launched an own-motion inquiry into Trade Me's update to its privacy policy. In November 2019, Trade Me had updated its privacy policy concerning members' ability to opt out of targeted advertisements. The update meant that Trade Me members could only opt out of third-party targeted advertising, so Trade Me could now target its own advertisements to members.

The inquiry found that Trade Me did not take reasonable steps in the circumstances to ensure that individuals understood the scope and nature of the advertising opt-out.

Businesses who wish to change their terms and conditions or privacy policies can adhere with the Privacy Act by considering:

- what individuals have been told about how their information will be used (and the substance and clarity of those communications);
- whether the new use is consistent or directly related to what individuals have been told or whether a new authority to use the information is needed; and
- whether they can provide individuals with options they need to maintain trust in their business e.g. can the business ring-fence information collected before the change occurred?

ICDPPC / Global Privacy Assembly award

The International Conference of Data Protection and Privacy Commissioners (ICDPPC) (now called the Global Privacy Assembly) consists of 122 privacy authorities from around the world.

In October 2019 at ICDPPC's 41st meeting in Tirana, Albania, we received an award in the Dispute Resolution and Enforcement Category for our inquiry and report into the Ministry of Social Development's misuse of its fraud investigation powers. The award was voted on by other privacy authorities. We were honoured to receive recognition from our international privacy protection peers.

Of the award the Commissioner said: "We are proud to have successfully advocated for the privacy rights of vulnerable members of New Zealand society. The inquiry and subsequent report show that personal information is about people. Misusing that information can cause measurable harm – especially to individuals who depend on the welfare system to support themselves and their families. These people are entitled to fairness in the system."

Privacy Trust Marks

Privacy Trust Marks are awarded by the Privacy Commissioner for products or services which demonstrate excellence in privacy and embrace the principles of privacy by design. A total of five marks have been awarded since the scheme was established in 2018.

We had six applications for Trust Marks this reporting year, of which two received the award.

The recipients were:

- Paperkite's Rippl contact tracing app
- Trust Integrity Compliance Company's Anti Money Laundering Customer Due Diligence Portal.

Policy

Covid-19 Public Health Response Act

In June 2020, the Privacy Commissioner submitted on the ex-post review of the COVID-19 Public Health Response Act 2020. It was sent to the Finance and Expenditure select committee following the passage of the Act under urgency. The Commissioner made a variety of recommendations on the operation of the Act, specifically in respect of the legal mechanisms enabling contact tracing.

The Commissioner submitted that in lieu of order-making powers under the COVID-19 Public Health Response Act, contact tracing provisions in the Health Act 1956 should be bolstered to deal with identified gaps in the contact tracing framework. The Select Committee have released their final report on the COVID-19 Public Health Response Act and recommended enduring legislation for health emergency responses, noting that the Health Act is outdated. We will continue to work with the Ministry of Health and other key stakeholders on these issues.

International app table and other Covid-19 work

Covid-19 resulted in a proliferation of technological solutions for contact tracing in New Zealand and internationally. Countries have implemented a variety of different tracing solutions with varying success.

We kept abreast of these developments, including monitoring evidence of the efficacy of various technological solutions and the privacy ramifications. We reviewed applications and other technology solutions that were being employed across the world and considered the privacy implications and implementation methods.

We also assisted the Ministry of Health with the NZ COVID Tracer app. We reviewed the privacy impact assessments for the initial deployment of the app and subsequent iterations, and provided privacy advice to Ministry officials.

Arms Legislation Bill

The Arms Legislation Bill was introduced partly as a response to the March 15 terrorist attack and as part of moves to modernise the more than 30-year-old Arms Act. The Bill established a registry for storing information about firearms and their holders, strengthened the firearms licensing regime and oversight of firearms holders and dealers, and established information sharing provisions to assist with the above.

We made several recommendations to Select Committee to improve the privacy outcomes of the Bill. These were:

- that the purpose of providing the Ministry of Foreign Affairs and New Zealand Customs Service with direct access to the registry of firearms be clarified to relate only to the movement of firearms across the border;
- that additional safeguards, such as audit and restrictions on further disclosure, be included in the provisions relating to direct access; and
- the requirement to consult the Privacy Commissioner on the drafting of regulations specifying the information to be included in the registry.

All our recommendations were accepted and reflected in the final Bill as passed by Parliament.

Terrorism Suppression (Control Orders) Bill

The Terrorism Suppression (Control Orders) Bill was introduced under urgency to implement measures to control a small number of individuals who may return or arrive in New Zealand and have participated in terrorism related activities overseas. The Bill implemented a civil regime of control orders to manage and monitor these individuals.

The control order regime allows the High Court to impose a control order if it is satisfied on the balance of probabilities that a person has engaged in or travelled to a foreign country to conduct terrorism-related activities, or has been deported from a country for terrorism-related reasons, and they pose a real risk of engaging in terrorism-related activities.

The restrictions the High Court could impose through a control order include:

- restricting an individual's movement, connectivity, access to information, ability to work and access to financial services
- monitoring and tracking the individual, collecting their biometric information and submitting them to drug and alcohol assessments.

We made a submission to Select Committee recommending that the Bill not proceed. We said we were not aware of any evidence involving such exceptional measures to justify significant intrusions into New Zealanders' privacy. We also noted that there were other legislative regimes that should and could be used, that a civil as opposed to a criminal regime was unjustified because of the highly intrusive powers; and that there was insufficient evidence that this Bill would be effective.

The Select Committee could not reach agreement on whether to recommend that the Bill be passed. Ultimately it passed.

Information sharing

Registrar-General / Police AISA

The Registrar-General of Births, Deaths and Marriages and the New Zealand Police entered into an Approved Information Sharing Agreement (AISA) in September 2019.

The AISA facilitates the provision of name change, non-disclosure direction and death information from the Department of Internal Affairs to the Police in order to improve accuracy of information held by Police.

The AISA enables Police to update the National Intelligence Application (NIA) to:

- link multiple identities to one individual
- update records of individuals in NIA
- detect and correct false information provided by individuals
- protect the identity of individuals who have a non-disclosure direction in force.

The AISA will allow name change, non-disclosure direction and death information to be shared beyond those reasons authorised by the statutes under which personal information was collected and on a regular and wholesale basis.

The sharing will not include information regarding:

- pre-adoptive birth registrations
- pre-sexual assignment or reassignment birth registrations
- non-disclosure directions made under the Domestic Violence Act 1995.

We were satisfied that the agreement would result in positive benefits outweighing the costs of sharing the information.

Customer Nominated Services AISA

We were engaged with the Department of Internal Affairs' (DIA) work on the Customer Nominated Services AISA. The Customer Nominated Services AISA is an Agreement executed between DIA, the Registrar-General, Births, Deaths and Marriages, and several other government agencies.

It enables information sharing to assist with the provision of public services that the individual has chosen to apply for, where the delivery of those services is supported by identity information held by DIA or the Registrar-General, or the services are provided by either DIA or the Registrar-General.

This AISA replaces multiple existing information matching agreements. It reduces multiple requests for the same information by different government agencies and removes the need to provide physical copies of information. It also improves the quality and consistency of information that agencies hold about an individual and makes it easier to detect issues such as identity fraud.

The Terrorism Suppression (Control Orders) Bill was introduced under urgency to implement measures to control a small number of individuals who may return or arrive in New Zealand and have participated in terrorism related activities overseas.



Outreach

We are committed to meeting and raising awareness of privacy issues with people around New Zealand. Our outreach activities include producing fortnightly newsletters, blogs and other guidance, hosting public events and sharing topical privacy content across social media channels. This reporting year, the Communications team's main focus was the promotion of the new Privacy Act.

Impact of Covid-19

The Covid-19 pandemic, associated lockdown and closure of New Zealand's border adversely impacted many of our in-person outreach activities. Our total number of presentations for this reporting period was 89, down 20% on last year. Many events we would have traditionally held or participated in were also cancelled.

Regional visits

The Privacy Commissioner routinely travels to regional centres around the country to strengthen our connections, disseminate key privacy messages and promote our resources.

The visits provide the Commissioner with the opportunity to speak and take questions from the public about the latest developments in privacy, and present to DHBs, local government, NGOs, and other groups.

In the reporting period, the Commissioner visited:

- Blenheim (September 2019)
- Kaikohe (November 2019)
- Christchurch (February 2020).

PrivacyLive

Prior to Covid-19, we held three PrivacyLive events in Auckland and Wellington.

These events are livestreamed and shared across social media to make them accessible to the broadest audience possible.

- Andelka Phillips – Your DNA is only a click away – 20 June 2019 (Auckland)
- Rachel Dixon (Office of the Victorian Information Commissioner) – Artificial Intelligence and its use in Government – 16 October 2019 (Wellington)
- Joëlle Jouret (European Data Protection Board) – GDPR in 2020 – 24 February 2020 (Auckland and Wellington)

Privacy Week

Privacy Week is an annual event (held in May) across the Asia-Pacific, organised by the Asia Pacific Privacy Authorities (APPA). We take the opportunity the week provides to raise awareness of privacy and data protection. We do this through a series of public talks and events.

This year's Privacy Week that had been scheduled to occur 11-15 May 2020 was postponed due to Covid-19. It was held on 2-6 November 2020. The new date gave us the opportunity to promote the Privacy Act 2020 before its 1 December commencement date.

Privacy Act podcast series

As part of our efforts to inform the public about the forthcoming changes to the Privacy Act, we recorded six short podcasts. The Privacy Commissioner and General Counsel used each episode to discuss a different aspect of the Act.

This podcast series can be accessed here: <https://privacy.org.nz/privacy-act-2020/resources/>

Privacy Good Research Fund

We launched The Privacy Good Research Fund in June 2015 to generate new knowledge in the areas of privacy and data protection.

In 2019, we received a grant from the International Association of Privacy Professionals Australia/ New Zealand Chapter (iappANZ) Legacy Fund, and sought additional support from the Social Investment Agency (SIA).

The fund had a total of \$75,000 available, with up to \$25,000 available for any single project. Twenty-one applications were received from New Zealand and abroad. The four successful applications were:

- an exploration of the way tech design influences users' privacy choices
- an investigation into how the Dunedin Study participants feel about their information being shared
- an examination of New Zealanders' attitudes to having smart speakers at home
- a look into whether New Zealand should adopt a US law requiring information held in the cloud about individuals be handed over for criminal investigations.

UMR Privacy Survey 2020

The Office of the Privacy Commissioner's survey – *Privacy Concerns and Sharing Data* – is a biennial snapshot of New Zealanders' attitudes to privacy and information sharing.

The survey was conducted by UMR Research between 31 March and 13 April and interviewed a nationally representative sample of 1,398 New Zealanders aged 18 years and older.

The survey found nearly two-thirds (65 percent) of survey respondents were in favour of more regulation of what companies can do with their customers' personal information.

The three top privacy concerns for New Zealanders interviewed for the survey were:

1. The unauthorised business sharing of their personal information (75 percent).
2. The theft of their banking details (72 percent).
3. The security of their personal information online (72 percent).

You can find a copy of the UMR Survey results here: <https://www.privacy.org.nz/assets/Privacy-concerns-and-sharing-data-OPC-reportApr-20.pdf>

Privacy Trust Mark

We launched the Privacy Trust Mark in May 2018 with the aim to give consumers assurances that a product or service has been designed with privacy in mind.

When assessing applications from organisations, we examine factors such as:

- has privacy been embedded into the design and is it a core value of the organisation?
- is the customer in control of their personal information?
- is there an ongoing commitment to improve privacy practice?

This year we awarded two new Trust Marks, bringing our total awarded to five. The first went to Trust Integrity Compliance's Anti-Money Laundering Customer Due Diligence Online Forms and AML Online Portal. The second was awarded to Paperkite's contact tracing app, Rippl.

We have received a total of 16 Trust Mark applications.





International

Due to Covid-19, many international events we would normally participate in were postponed or moved online. This reporting year, we attended two privacy forums, the Asia Pacific Privacy Authorities Forum (APPA) and the Global Privacy Assembly (GPA). Both were held in late 2019.

Asia Pacific Privacy Authorities Forum (APPA)

APPA is the principal forum for privacy authorities in the Asia Pacific region. We attended the 52nd Forum in Cebu, Philippines in December last year. Fourteen APPA authorities attended the two-day event. Key issues discussed at the forum included:

- closer ties between competition/consumer protection authorities and data protection authorities across the region
- facial recognition technology use by law enforcement
- ongoing modernisation of data protection laws
- risks of re-identification in anonymised datasets.

The 53rd forum was held in June 2020 via video conferencing due to Covid-19. We attended the three-day event, which had a large focus on personal data issues arising from Covid-19. We briefed APPA members on: the activation of the Civil Defence National Emergencies (Information Sharing) Code 2013; the amendment to the Telecommunications Information Privacy Code; and the implementation of the Privacy Bill, which is due to come into force in December this year. Other issues discussed at the 53rd forum included:

- data breach notifications
- biometrics and data protection
- appropriate regulations for artificial intelligence.

The next forum will be hosted by Australia's Office of the Victorian Information Commissioner in December 2020.

Global Privacy Assembly

We and around 120 other regulators attended the 41st gathering of the Global Privacy Assembly (formerly the ICDPPC) held in October 2019 in Tirana, Albania. During this meeting the organisation adopted a new name – Global Privacy Assembly – and a new strategic direction until 2021. The focus of the GPA was AI and ethics – building on the discussion at the 40th Conference.

We proposed a resolution on social media and violent extremist content online that was adopted. This resolution builds on the work of the Christchurch Call to Action. Some of the issues discussed included: the global privacy challenge of data driven business models; data protection and competition as converging digital regulation; Convention 108+; and future challenges facing regulators.

The Office of the Privacy Commissioner New Zealand is scheduled to host the GPA in 2022 in Auckland.

Other international activities

OECD working party on data governance and privacy

We have been participating remotely in the review of the OECD Privacy Guidelines 2013. For more than a year, the Privacy Experts Group has been reviewing whether the OECD Privacy Guidelines need updating to match our fast-paced, digitally driven world. The working party has also examined data breach reporting, data portability and, recently, the impacts of Covid-19 on privacy and data protection.

Covid taskforce

During May and June, we participated in several meetings as a member of the Global Privacy Assembly's COVID-19 Taskforce.

These meetings were intended to drive practical responses to privacy issues emerging from the pandemic and for data protection and privacy authorities to share information and best practice.

Our Office attended three meetings, where we provided advice to other members on New Zealand's experience surrounding the sharing of health information during the pandemic. We also attended a workshop in April held by the GPA and OECD – addressing the data governance and privacy challenges in the fight against Covid-19. We also shared resources that we prepared on Covid-19 with the Taskforce and members.

Global Privacy Enforcement Network (GPEN)

GPEN continues to be a key means of connecting with our international counterparts. We participate in monthly GPEN Pacific teleconferences and in the annual GPEN sweep, a coordinated global research project.

In 2019, we managed and coordinated the GPEN sweep, looking at how organisations handle and respond to data breaches. Given the mass of information that is collected and held by organisations, it is inevitable that at certain times personal information will be accessed, disclosed, or otherwise acquired in a way that is not authorised. How an organisation responds to a data breach incident (including both notification as a response and steps taken to prevent future breaches) is of key importance to data protection authorities (DPAs), and the individuals whose personal information is affected.

Sixteen DPAs participated in the sweep in 2019, contacting a total of 1,145 organisations worldwide. Participating DPAs were asked to reach out to organisations with a set of pre-determined questions which focused on their current practices for recording and reporting data breaches.

Ongoing review of EU adequacy

We provided ongoing assistance to Ministry of Justice officials regarding the current review of New Zealand's EU adequacy status. We met with European Commission officials via video conference and provided advice and responses to questions raised in the review about the operation of New Zealand's privacy laws.

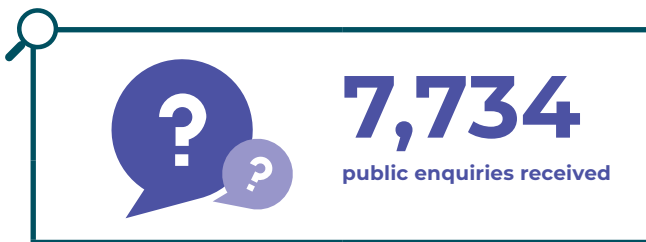
We provided our 11th periodic update report to the European Commission covering the period January – June 2020, including passage of the new Privacy Act 2020.

For more than a year, the Privacy Experts Group has been reviewing whether the OECD Privacy Guidelines need updating to match our fast-paced, digitally driven world.

Enquiries and education

This year we dealt with 7,734 public enquiries, a slight decrease from the 7,947 enquiries we received during the last reporting period.

Of the total, 3,579 enquiries came through the call centre – an average of 300 a month. Of these calls, a fifth were referred through to our staff. We aim for the call centre to deal with straightforward questions, with our staff available to provide more in-depth assistance as required.



AskUs

AskUs is the FAQ section of our website and one of the main avenues for us to address public privacy questions. It is one of the most viewed sections of our website.

The three most popular questions searched on AskUs are:

1. What is personal information?
2. Can I record someone without telling them?
3. Are there rules regarding where CCTV cameras can be placed?

Live chat

Our website normally features a live chat function to enable the public to engage directly with us about their privacy issues. This service was suspended in March 2020 when lockdown began but resumed operation in September.

Website

Our website received slightly less than half a million visits between the period 1 July 2019 and 30 June 2020. There was a spike in visits in April 2020, associated with lockdown.

Media

In the past year we received 291 media enquiries representing an 11% drop from the 327 enquires in 2018/19.

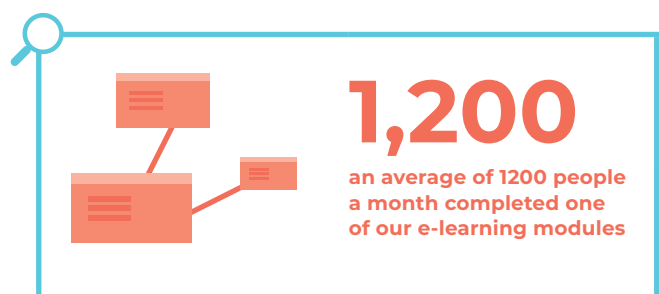
There were several issues that generated significant media interest during the past reporting year. In addition to several high-profile privacy breaches, the MSD wage subsidy register, Covid-19 contact tracing apps, Privacy Act 2020, and the use of facial recognition technology by government agencies all attracted considerable media attention.



Online learning modules

Our e-learning modules are a popular resource that help thousands of New Zealanders every year understand their rights and responsibilities under the Privacy Act. This year we released one new e-learning module, *Privacy ABC for Schools*, which provides an overview of how the Privacy Act is applied in the context of schools.

We now offer 11 education modules. Approximately 1,200 people complete one of our modules every month. By the end of this reporting year, more than 33,000 people had completed one of our e-learning courses.



Breach notifications

We receive privacy breach notifications (also known as data breaches) from a variety of public and private sector organisations.

Under the Privacy Act 1993, notifying the Privacy Commissioner of privacy breaches was voluntary. However, we encouraged organisations to report their breaches to us. Notifications help us identify common privacy issues and risks. We use the lessons learned from these breaches to develop education resources and FAQs.

Getting ready for mandatory breach notifications

Under the Privacy Act 2020, from 1 December it is mandatory for organisations to report privacy breaches that may cause or have caused someone serious harm to the Privacy Commissioner and affected individuals.

To make it easy for organisations to report their breaches to us, we developed the NotifyUs tool. The tool will help organisations know whether their breach is notifiable and guide them through the notification process. Letting people know their privacy has been breached allows them the opportunity to take steps to secure their personal information, lessening the chance of them experiencing serious harm.

From 1 December 2020, we anticipate the volume of breaches reported to us to substantially increase. Countries that have implemented similar breach regimes to New Zealand, such as Australia and Ireland, experienced a five to seven-fold increase in the number of reported breaches in the year following the introduction of their new regimes.

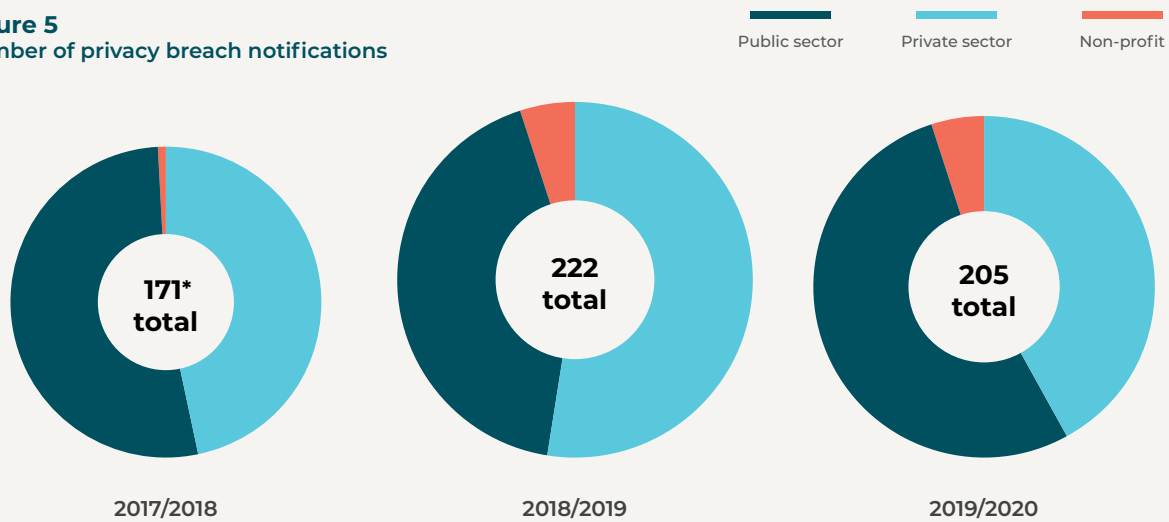
This year we received 205 breach notifications. Of these, 109 came from public agencies, 86 from private organisations and 10 from non-profit organisations.

Because breach reporting was voluntary, during the reporting year there was no way of knowing what proportion of all the breaches that occurred were reported to our office.

The number one type of breach reported to us by organisations relates to human error, e.g. employees of an organisation sending someone's personal information to the wrong person.

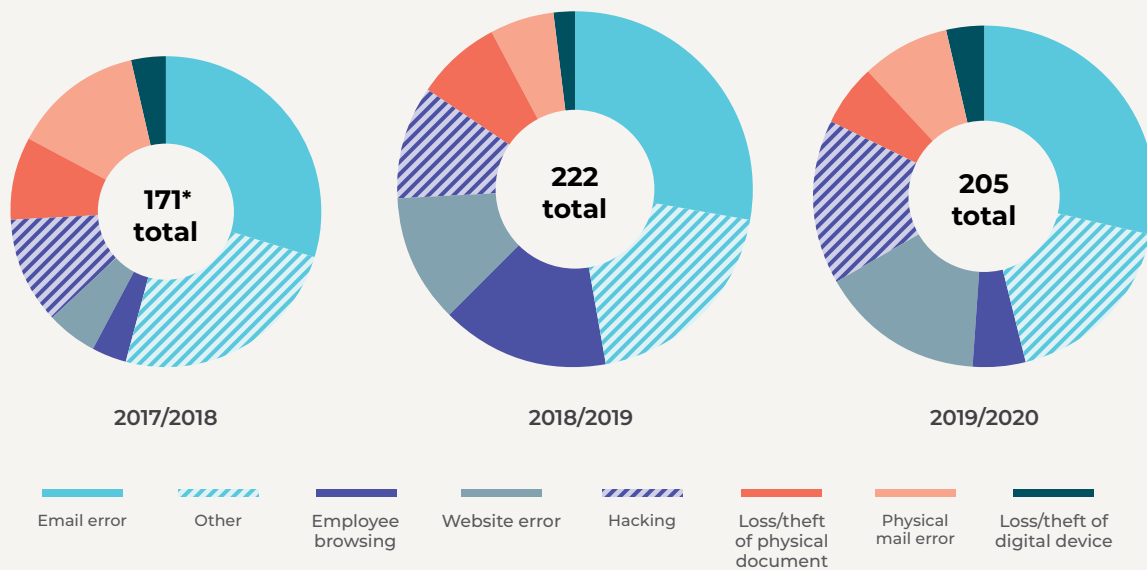


Figure 5
Number of privacy breach notifications



*This figure has been adjusted up from 168 following a data cleansing exercise.

Figure 6
Common types of breaches



Note: more than one type of information may be involved in a breach.
*This figure has been adjusted up from 168 following a data cleansing exercise.

Information matching

Statutory review of information matching provisions

The Privacy Act requires that the Commissioner review the operation of each information matching provision every five years. In these reviews under s. 106 the Commissioner recommends whether a provision should continue, be amended or be cancelled.

This year the Commissioner issued three reports reviewing information matching provisions.

Ministry of Social Development international social welfare reciprocity agreements

This report covered three provisions that are relied upon for international social welfare provision reciprocity arrangements with Australia, Malta, the Netherlands and the United Kingdom.

The Commissioner recommended that those provisions continue, with the amendments to the Social Security Act provision that were included in the Privacy Bill.

- Social Security Act 2018 section 380
- Customs and Excise Act 2018 section 309
- Tax Administration Act 1994 Schedule 7 Part C Subpart 2 clause 45

Ministry of Social Development information matching; review of statutory authorities for information matching

This report covered seven provisions that are relied upon for social welfare activities. The Commissioner recommended that those provisions continue, except for the Customs and Excise Act 2018, section 308 provision which was superseded by an information sharing agreement in May 2019 and should be repealed.

- Accident Compensation Act 2001, section 281
- Births, Deaths, Marriages, and Relationships Registration Act 1995, section 78A
- Corrections Act 2004, section 180
- Customs and Excise Act 2018, section 308
- Education Act 1989, section 226A and section 235F
- Education Act 1989, section 307D
- Social Security Act 2018, schedule 6 clause 13

Accident Compensation Corporation, Department of Internal Affairs, and Ministry of Business, Innovation and Employment (Motor Vehicle Traders Register) information matching

This report covered five provisions that are relied upon by three agencies for their activities. The Commissioner recommended that those provisions continue, except for the *Citizenship Act, 1977* section 26A provision which was superseded by an information sharing agreement and should be repealed.

- Accident Compensation Act 2001, section 246 and Tax Administration Act 1994 Schedule 7 Part C subpart 2 clause 41 and 42
- Accident Compensation Act 2001 section 280
- Citizenship Act 1977 section 26A
- Motor Vehicle Sales Act 2003 section 120 and 121
- Motor Vehicle Sales Act 2003 section 122 and 123

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

¹ The programme was not operated during the review year.

Changes in authorised and operating programmes

Currently operating:

There were 47 information matching programmes in operation, and six programmes that were not active. The Commissioner assessed one programme as being not compliant with the requirements intended to protect the individuals affected by the programmes as they commenced online transfer of the information before seeking approval. Other programmes temporarily used online transfers during the period of the Covid-19 lockdown.

New provisions and programmes:

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

Programmes suspended:

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

The Ministry of Education did not operate its programme with the DIA for birth records but is 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 its 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 is considering alternative approaches to receiving the information (Immigration Act 2009, section 295).

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

MSD also did not need to use the provision to allow Inland Revenue to respond to tax information enquiries 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, Schedule 7 clause 45).

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

Programmes ceasing:

As advised last year, four of the current information matches between different functions of the Department of Internal Affairs are being replaced by new processes conducted under an Approved Information Sharing Agreement. The "Information Sharing Agreement between the Department of Internal Affairs and the Registrar-General, Births, Deaths and Marriages" was authorised by an Order-in-Council on 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 its work processes and systems. When these changes are complete, they will operate the information sharing under the AISA.

- Citizenship/DIA Passports
- BDM/DIA Passports
- BDM Births & Marriages/Citizenship applications
- Citizenship/BDM Citizenship by Birth

Parliament passed no new information matching provisions during the year.

Office and functions



Independence and competing interests

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

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

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

Reporting

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 Assistant Commissioner (Policy & Operations) is responsible for investigations and dispute resolutions, enquiries, policy and technology advice, and information matching work.

The Public Affairs Manager is responsible for our communications, education, publications, media and external relations functions.

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 in the area of investigations and Privacy Act law reform.

Covid-19

The Covid-19 pandemic affected the Office and functions of the Privacy Commissioner from March 2020.

Our IT architecture was shaped by the lessons of the Kaikōura earthquake and the consequent need to be able to work remotely for extended periods. We maintain business continuity of systems through the move to cloud-based servers on the Microsoft Azure platform in Sydney. We use Office 365 software for operational matters and our electronic document records management system as our documents of record providing access to all official 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 2017-2021. The policy encourages active staff participation in all EEO matters. We review the policy annually, together with policies on recruitment, employee development, harassment prevention, and health and safety.

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

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

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

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

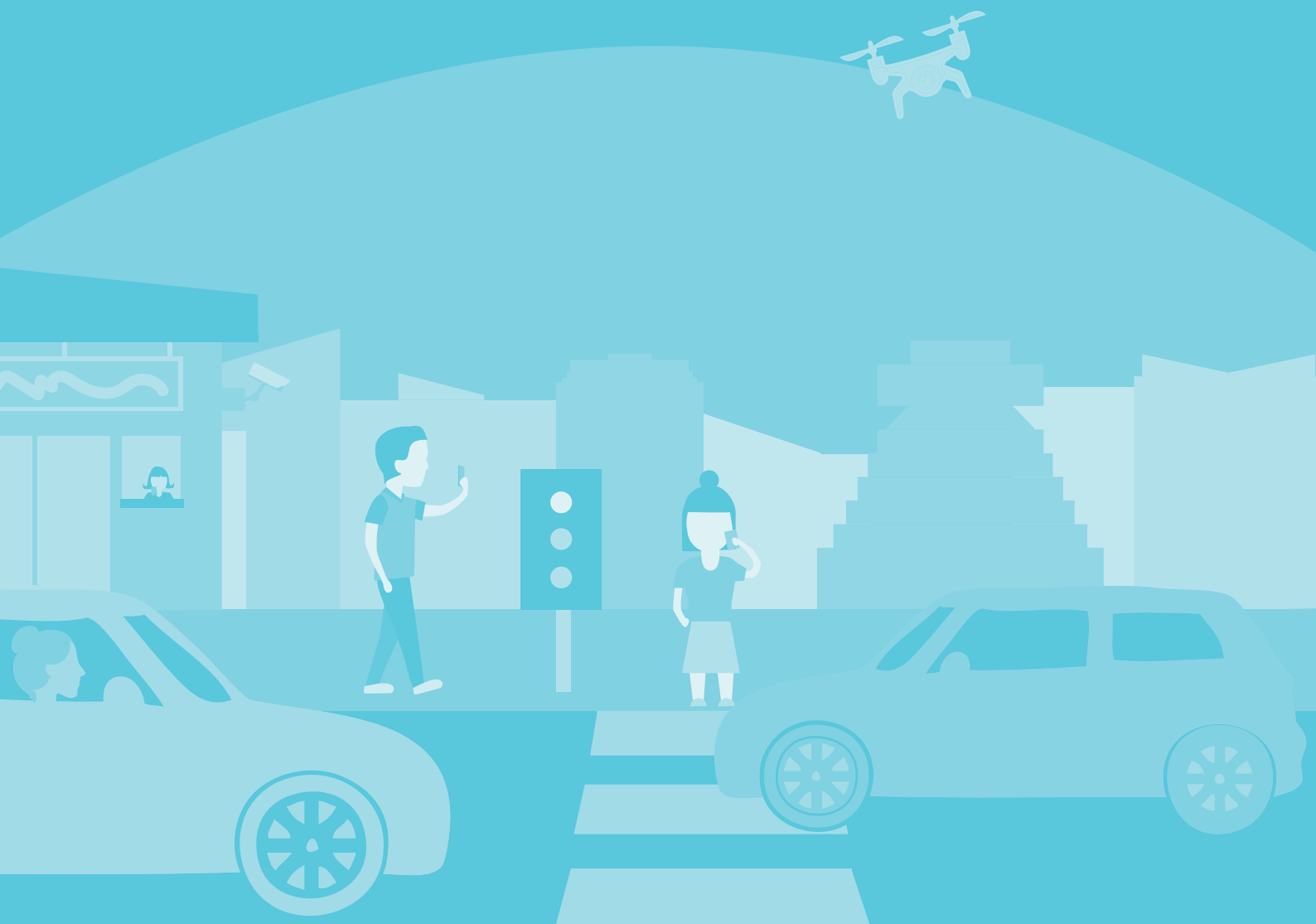
We have formal policies regarding bullying, harassment, and the provision of a safe and healthy workplace. Staff have ready access to external support through our employee assistance programme.

Workplace gender profile

as at 30 June 2020

Role	Women		Men		Total
	Full-time	Part-time	Full-time	Part-time	
Commissioner			1		1
Senior managers	2		1		3
Team and unit managers	2		1		3
Investigations and Dispute Resolution	4	2	3		9
Administrative support	5	2			7
Policy	4		1	1	6
Communications			3		3
Legal	2				2
Total	19	4	10	1	34

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

In the opinion of the Privacy Commissioner, these financial statements and statement of performance fairly reflect the financial position and operations of the Privacy Commissioner for the year ended 30 June 2020.



J Edwards
Privacy Commissioner
4 December 2020



G F Bulog
General Manager
4 December 2020



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 2017-2021 identifies three high level outcomes to support our vision to “make privacy easy”. The “Working towards our strategic goals” section of this Annual Report has provided an overview of the work we have undertaken this reporting year to support our progress towards these outcomes.

The Statement of Performance Expectations for the year to June 2020 identified four output classes to support these three outcomes. These have remained consistent with previous years. We report our progress against these output areas in this section and have linked through to the outcomes where appropriate using the following symbols:-

-  **Outcome 1** – Increased citizen and consumer trust in the digital economy
-  **Outcome 2** – Innovation is promoted and support
-  **Outcome 3** – Increased influence to improve personal information practices

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 2020 was limited. We recently upgraded our IT systems meaning staff could 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.

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	5,582	5,708
Other revenue	242	323
Total revenue	5,824	6,031

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 operating grant achievement included \$126k towards Privacy Act implementation costs. This had been included in the budget for the previous financial year on the assumption that the law reform would have progressed to enactment. This did not occur in the 2019 financial year and so this funding was received in the 2020 year instead.

The achievement amount above was increased from the original appropriation by \$738k to \$5,708k to provide for the implementation of the new Privacy Act. The amount received by the Privacy Commissioner equates to 1.6% of the total Vote Justice Non-Departmental Output Expenses Appropriation for 2019/20. The total expenses in the year are \$5,911k as set out in the cost of service statement below.

Cost of service statement

for the year ended 30 June 2020

As set out in the 2019/20 Statement of Performance Expectations, the Privacy Commissioner committed to provide four output classes. The split of funds across these four output classes is set out below:

	Actual 2020 \$000	Budget 2020 \$000	Actual 2019 \$000
OUTPUT CLASS 1: GUIDANCE, EDUCATION AND AWARENESS			
Resources employed			
Revenue	924	958	818
Expenditure	865	926	748
Net surplus/(deficit)	59	32	70
OUTPUT CLASS 2: POLICY AND RESEARCH			
Resources employed			
Revenue	2,230	2,167	1,900
Expenditure	2,283	2,186	2,098
Net surplus/(deficit)	(59)	(19)	(198)
OUTPUT CLASS 3: INFORMATION SHARING/MATCHING			
Resources employed			
Revenue	778	751	783
Expenditure	669	633	729
Net surplus/(deficit)	109	118	54
OUTPUT CLASS 4: COMPLIANCE			
Resources employed			
Revenue	2,099	1,948	1,720
Expenditure	2,094	1,953	1,850
Net surplus/(deficit)	5	(5)	(130)
TOTALS			
Resources employed			
Revenue	6,031	5,824	5,221
Expenditure	5,911	5,698	5,425
Net surplus/(deficit)	120	126	(204)

The following tables set out the assessment of our performance against the targets 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





Output class 1: Guidance, education and awareness

Why this is important

One of our functions is to promote individual privacy. Outreach to the public and business is a major focus and includes an active programme of seminars, presentations and regional outreach visits, as well as responding to enquiries from the public, media and businesses. Over the period covered by the Statement of Intent, there is a specific focus on reaching out to diverse communities. We also produce a range of guidance and other resource material.




During the reporting year, we increasingly used our website to provide these services online. One new e-learning module went “live” during the year – Privacy for Schools.

Output Measures

Measure	Estimate	Achieved 2019/20	Achieved 2018/19
Quantity			
Number of people completing education modules on the online system. 	5,000	Achieved 12,725 people have completed e-learning modules in the year to 30 June 2020. ¹	Achieved – 10,326
Presentations at conferences and seminars. 	90	Substantially achieved – 89	Achieved – 112
Public enquiries received and answered. 	8,500 ²	Not achieved – 7,734 Public enquiries are externally driven and will fluctuate between years.	Achieved – 7,947
Media enquiries received and answered. 	250	Achieved – 291	Achieved – 327

¹ This is measured by the number of modules completed. One person may complete multiple modules during the year.

² This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation and was the same as the SPE target.

Measure	Estimate	Achieved 2019/20	Achieved 2018/19
Quality			
The Office actively engages in and has proactively established multi-stakeholder relationships both nationally and internationally. 	Achieved	Achieved Despite the impacts of Covid-19, we continued our engagement both nationally and internationally. See the Outreach section for further information.	Not applicable – this is a new measure for 2019/20.
The percentage of respondents to the annual stakeholder survey who indicate, where applicable, that the guidance materials reviewed on the website were useful and met their needs. 	85%	Achieved – 89%³	Achieved – 96%
Timeliness			
Respond to all enquiries within two working days. 	95% ⁴	Substantially achieved – 93%	Not achieved – 92% ⁵

³ The satisfaction rate is measured as a simple ratio of the fifth question in the Office's annual external stakeholder survey run through SurveyMonkey. There were 53 responses to this question. SurveyMonkey has some limitations. Records can be deleted and modified, and the reported result may not be completely free from error.

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



⁵ The prior year target was set at 100% rather than 95%. Against the prior year target the achievement was "Not achieved".



Output class 2: Policy and research

Why this is important

We actively comment on legislative, policy or administrative proposals that affect privacy to make sure the proposals take the Privacy Act's requirements into account. We are also actively involved in international meetings. This gives us the ability to identify and respond to emerging issues in a timely manner.

Output Measures

Measure	Estimate	Achieved 2019/20	Achieved 2018/19
Quantity			
The number of consultations, submissions and office projects completed in the year. 	150	Achieved – 151 The number of consultations is demand driven through external organisations.	Not achieved – 116
Identifiable progress in international efforts in which we are actively engaged to work towards more sustainable platforms for cross border cooperation. 	Achieved	Achieved The Office contributed to the work Global Privacy Assembly COVID-19 Taskforce, the OECD Data Governance and Privacy group, the Asia-Pacific Privacy Authorities forum, United Nations Global Pulse and Asian-Business Law Institute.	Achieved

Measure	Estimate	Achieved 2019/20	Achieved 2018/19
Quality			
<p>Our participation in the law reform process is valued by the Ministry of Justice.</p> 	Achieved	<p>Achieved</p> <p>The Ministry of Justice has provided feedback noting that the expert and operational input from the Office is of high quality and valuable.</p> <p>The responses for input were also timely and were delivered within agreed timelines.</p>	Achieved
<p>The percentage of externally reviewed policy, information sharing and information matching files that are rated 3.5 out of 5 or better for quality.</p> 	85%	<p>Achieved – 89%</p> <p>Based on findings from an independent review of a sample of files closed in the year.</p>	Achieved – 92%
Timeliness			
The percentage of policy files where advice was delivered within agreed timeframes	95%	Achieved – 99%	Substantially achieved – 95% ⁶






⁶ The target in the prior year was set at 100% and not 95%.

Output class 3: Information sharing and matching

Why this is important

We have statutory roles in overseeing authorised information matching programmes (Part 10 of the Privacy Act) and approved information sharing agreements (Part 9A of the Privacy Act). We also provide advice to agencies carrying out information sharing and matching about how to meet their responsibilities under Part 9A and Part 10 respectively.

Output Measures

Measure	Estimate	Achieved 2019/20	Achieved 2018/19
Quantity			
The number of new Approved Information Sharing Agreements received for consultation under section 96O of the Privacy Act 	4	Not achieved – 0 The number of agreements is demand driven through external organisations.	Achieved – 2 ⁷
The number of formal reports produced that relate to information sharing or information matching programmes, under sections 96P, 96X, 96O or 106 of the Privacy Act  	8	Not achieved – 4	Not achieved – 4
The number of proposals consulted on involving information sharing or matching between government agencies, completed during the year.  	30	Not achieved – 22	Substantially achieved – 29
Timeliness			
The percentage of information sharing and matching files where advice was delivered within agreed timeframes	100%	Substantially achieved – 96%	Achieved – 100%

⁷ The prior year target was set at 2 compared to 4 for the current year.

Output Class 4: Compliance







Why this is important

Another of our core functions is the provision and management of an independent and responsive complaints and investigation process. We continue to transform the way we deal with complaints, with a focus on more timely resolutions. In the year, 42% of all complaints were lodged using the online complaints lodgement system.

The new NotifyUs tool, which was still being developed at the end of the year, will be one of the main ways organisations report privacy breaches to us in future.

We also review and amend codes of practice.

Output Measures

Measure	Estimate	Achieved 2019/20	Achieved 2018/19
Quantity			
Number of complaints received 	800	Not achieved – 691 The number of complaints received is externally driven.	Not achieved – 793
Number of data breach notifications received 	200	Achieved – 205	Achieved – 222
Quality			
The percentage of complaints files closed by settlement between the parties 	40%	Achieved – 64%	Achieved – 57%
Amendments to Codes of Practice meet all statutory requirements 	100%	Achieved The Commissioner has consulted on an amendment to the Telecommunications Information Privacy Code 2003.	Achieved
The percentage of externally reviewed complaints investigations that are rated as 3.5 out of 5 or better for quality. 	85%	Achieved – 95% Based on the results of an external review of a sample of complaints files closed between July 2019 and June 2020.	Achieved – 98%
Timeliness			
The percentage of open files greater than 6 months old at year end. 	10%	Not achieved – 11%	Not achieved – 13%

Statement of accounting policies

for the year ended 30 June 2020

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 2020 and were approved by the Commissioner on 4 December 2020. The financial statements cannot be altered after they have been authorised for issue.

Basis of preparation

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

Statement of compliance

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

The financial statements have been prepared in accordance with Tier 2 PBE accounting standards. The Tier 2 criteria have been met as expenditure is less than \$30m and the Privacy Commissioner is not publicly accountable (as defined in XRB A1 Accounting Standards Framework).

These financial statements comply with PBE accounting standards.

Measurement base

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

Functional and presentation currency

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

Summary of significant accounting policies

Significant accounting policies are included in the notes to which they relate.

Significant accounting policies that do not relate to specific notes are outlined below.

Budget figures

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

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

Cost allocation

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

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

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

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

Goods and Services Tax (GST)

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

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

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

Commitments and contingencies are disclosed exclusive of GST.

Income tax

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

Financial instruments

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

Critical accounting estimates and assumptions

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

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

- useful lives and residual values of property, plant and equipment – refer to Note 9
- useful lives of software assets – refer to Note 10.

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 2020:

- 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 2020

	Note	Actual 2020 \$000	Budget 2020 \$000	Actual 2019 \$000
Revenue				
Crown revenue	2	5,708	5,582	4,970
Other revenue	2	323	242	251
Total income		6,031	5,824	5,221
Expenditure				
Promotion	4	124	223	120
Audit fees		33	31	32
Depreciation and amortisation	4,9,10	201	250	221
Rental expense		396	398	420
Operating expenses	4	891	811	933
Contract services		648	246	259
Staff expenses	3	3,618	3,739	3,440
Total expenditure		5,911	5,698	5,425
Surplus/(deficit)		120	126	(204)
Other comprehensive revenue and expenses		-	-	-
Total comprehensive revenue and expenses		120	126	(204)

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 2020

	Note	Actual 2020 \$000	Budget 2020 \$000	Actual 2019 \$000
Total equity at the start of the year		976	1,170	1,180
Total comprehensive revenue and expenses for the year		120	126	(204)
Total equity at the end of the year	5	1,096	1,296	976

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 2020

	Note	Actual 2020 \$000	Budget 2020 \$000	Actual 2019 \$000
Public equity				
General funds	5	1,096	1,296	976
Total public equity		1,096	1,296	976
Current assets				
Cash and cash equivalents	6	1,093	1,033	840
Receivables	7	187	30	99
Inventory	8	-	15	16
Prepayments	7	105	50	86
Total current assets		1,385	1,128	1,041
Non-current assets				
Property, plant and equipment	9	204	175	285
Intangible assets	10	109	297	151
Capital work in progress	9, 10	82	-	-
Total non-current assets		395	472	436
Total assets		1,780	1,600	1,477
Current liabilities				
Payables	11	338	124	269
Employee entitlements	13	317	180	220
Total current liabilities		655	304	489
Non-current liabilities				
Lease incentive	12	29	-	12
Total non-current liabilities		29	-	12
Total liabilities		684	304	501
Net assets		1,096	1,296	976

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

Statement of cash flows

for the year ended 30 June 2020

	Actual 2020 \$000	Budget 2020 \$000	Actual 2019 \$000
CASH FLOWS FROM OPERATING ACTIVITIES			
Cash was provided from:			
Receipts from the Crown	5,708	5,582	4,970
Receipts from other revenue	179	211	225
Interest received	11	30	27
Cash was applied to:			
Payments to suppliers	2,033	1,729	1,781
Payments to employees	3,521	3,738	3,423
Net Goods and Services Tax	1	(20)	(21)
Net cash flows from operating activities	343	376	39
CASH FLOWS FROM INVESTING ACTIVITIES			
Cash was applied to			
Purchase of property, plant and equipment and intangibles	90	275	250
Cash was provided from			
Sale of property, plant and equipment and intangibles	-	-	-
Net cash flows from investing activities	90	275	250
Net increase/(decrease) in cash held	253	101	(211)
Plus opening cash	840	932	1,051
Closing cash balance	1,093	1,033	840
Cash and bank	1,093	1,033	840

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 2020

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 lower than the budgeted surplus by \$6k. This is primarily due to the following:

Operating grant (up on budget by \$126k)

The \$126k Privacy Act Implementation Costs contingency funding was received in the current year rather than the prior year as originally budgeted.

Other income (up on budget by \$100k)

Additional income was received in the year towards the costs of updating the Telecommunications Information Privacy Code and funding the Privacy Good Research Fund.

Staff expenses (down on budget by \$121k)

There have been several staff vacancies as a result of staff departures during the year. Of particular note, two members of the senior leadership team left the Office. One of the roles was filled later in the year and the other role is currently being filled by a contractor. Staff development costs were also less than anticipated, partly due to the impact of Covid-19.

Contract services (up on budget by \$402k)

The most significant costs in the year relate to work associated with the new Privacy Act including project management and strategy development, Code amendments and research for the new Breach Reporting tool. This makes up approximately \$346k of the total costs. Additional contractors were also brought in to cover for staff vacancies as noted above – this covers approximately \$183k of the total cost.

Depreciation and amortisation (down on budget by \$49k)

The cost of additions during the year has been significantly less than budgeted resulting in lower than anticipated depreciation.

Other operating expenses (up on budget by \$80k)

The three main areas which are over budget for the year are computer maintenance costs (over by \$101k), software licensing costs (over by \$43k) and research projects (over by \$62k). The increases in both computer maintenance and licensing costs are mainly due to monthly costs coming in higher than anticipated, coupled with additional costs associated with the Auckland Office refurbishment and Covid-19 related costs. The Research costs relate to the Privacy Good Research Fund which had not been budgeted for in the 2020 year.

In addition, there were several areas that are below budget. The most significant was staff development, recruitment, litigation and domestic travel. These areas account for a decrease of \$128k.

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 the 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 the 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 (2019: \$nil).

Other revenue breakdown

	Actual 2020 \$000	Actual 2019 \$000
Other grants received	161	161
Forums and conferences	-	60
Other revenue	151	-
Interest revenue	11	30
Total other revenue	323	251

Note 3: Staff expenses

Accounting policy

Superannuation schemes

Defined contribution schemes

Obligations for contributors to KiwiSaver 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 2020 \$000	Actual 2019 \$000
Salaries and wages	3,384	3,302
Employer contributions to defined contribution plans	101	97
Other staff expenses	36	33
Increase/(decrease) in employee entitlements	97	8
Total staff expenses	3,618	3,440

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	Actual 2020 \$000	Actual 2019 \$000
\$100,000 – \$109,999	3	
\$110,000 – \$119,999	1	
\$120,000 – \$129,999	1	3
\$130,000 – \$139,999	1	1
\$140,000 – \$149,999	2	1
\$150,000 – \$159,999	1	
\$160,000 – \$169,999		1
\$170,000 – \$179,999	2	1
\$180,000-\$189,999		1
\$190,000-\$199,999		
\$320,000-\$329,999		
\$330,000-\$339,999		
\$340,000-\$349,999	1	1

No redundancy payments were made in the year (2019: \$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 2019 to 30 June 2020.

Name	Position	Amount 2020	Amount 2019
John Edwards	Privacy Commissioner	346,000	343,373

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 \$62k was expensed in relation to these grants in 2020 (2019: \$nil).

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 2020 \$000	Actual 2019 \$000
Fees paid to auditors:		
External audit – current year	33	32
Promotion costs:		
Website development expenses	96	26
Privacy Forum	-	8
Conferences	-	61
Other marketing expenses	28	26
Total promotion expenses	124	120
Depreciation and amortisation:		
Furniture and fittings	90	86
Computer equipment	33	33
Office equipment	9	11
Intangibles	69	91
Total depreciation and amortisation	201	221
Rental expense on operating leases	396	420
Contract services	648	259
Other operating expenses:		
Computer maintenance/licences	281	202
Staff travel	120	153
Staff development	33	84
Loss on disposal	-	2
Grant expenditure	62	-
Recruitment	18	86
Utilities	209	221
Other	168	185
Total other operating expenses	891	933

Operating leases as lessee

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

	Actual 2020 \$000	Actual 2019 \$000
Not later than one year	317	338
Later than one year and not later than five years	549	654
Later than five years	58	169
Total non-cancellable operating leases	924	1,161

The Privacy Commissioner leases two properties, one in Wellington and the other in Auckland. The Wellington lease was re-negotiated in 2015 and will expire in February 2021. The Auckland lease was re-negotiated in 2019 and will expire in December 2025.

Lease incentives were offered as part of the negotiation of both leases. These are 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 2020 \$000	Actual 2019 \$000
Opening balance	976	1,180
Net surplus/(deficit)	120	(204)
Closing balance	1,096	976

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 2020 \$000	Actual 2019 \$000
Cash on hand and at bank	243	71
Cash equivalents – on call account	850	769
Total cash and cash equivalents	1,093	840

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 2020 \$000	Actual 2019 \$000
Receivables	187	99
Prepayments	105	86
Total	292	184

Total receivables comprise:

GST receivable (exchange transaction)	51	50
Other receivables (non-exchange)	136	49
Total	187	99

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 (2019: \$nil).

Note 8: Inventories

Accounting policy

Inventories held for distribution, or consumption in the provision of services, that are not issued on a commercial basis are measured at cost.

Inventories held for sale or use in the provision of goods and services on a commercial basis are valued at the lower of cost and net realisable value. The cost of purchased inventory is determined using the weighted average cost method.

The write-down from cost to current replacement cost or net realisable value is recognised in the statement of comprehensive revenue and expenses in the period when the write-down occurs.

	Actual 2020 \$000	Actual 2019 \$000
Publications held for sale	-	1
Publications held for distribution	-	15
Total inventories	-	16

Inventories were written down by \$16k (2019: \$nil) to \$nil during the year. Inventories were assessed as being obsolete due to the enactment of the new Privacy Act which will result in the need to update relevant publications.

No inventories are pledged as security for liabilities (2019: \$nil).

Note 9: 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; and
- analysis of prior asset sales.

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

Breakdown of property, plant and equipment and further information

	Furniture and fittings \$'000	Computer equipment \$'000	Office equipment \$'000	Total \$'000
Cost				
Balance at 1 July 2018	785	295	64	1,144
Additions	-	78	60	138
Disposals	-	(209)	(48)	(257)
Balance at 30 June 2019	785	164	76	1,025
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
Accumulated depreciation and impairment losses				
Balance at 1 July 2018	541	250	54	845
Depreciation expense	86	33	11	130
Disposals	-	(205)	(30)	(235)
Balance at 30 June 2019	627	78	35	740
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
Carrying amounts				
At 30 June and 1 July 2019	158	86	41	285
At 30 June 2020	95	76	33	204

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

Capital commitments

The Privacy Commissioner has capital commitments of \$nil as at 30 June 2020 (2019: \$nil).

Work in progress

The capital work in progress figure is \$nil as at 30 June 2020 (2019: \$nil).

Note 10: 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 9. 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 two interactive databases that went live in mid-2016 and seven interactive e-learning tools. The tools were developed by an external provider. These tools have a finite life, which requires the Office to estimate the useful lives 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.

Movements for each class of intangible asset are as follows:

	Acquired software \$000	Interactive tools \$000	Total \$000
Cost			
Balance at 1 July 2018	72	204	276
Additions	133	39	172
Disposals	(72)	-	(72)
Balance at 30 June 2019	133	243	376
Balance at 1 July 2019	133	243	376
Additions	12	15	27
Disposals	-	-	-
Balance at 30 June 2020	145	258	403
Accumulated amortisation and impairment losses			
Balance at 1 July 2018	72	134	206
Amortisation expense	29	62	91
Disposals	(72)	-	(72)
Balance at 30 June 2019	29	196	225
Balance at 1 July 2019	29	196	225
Amortisation expense	41	28	69
Disposals	-	-	-
Balance at 30 June 2020	70	224	294
Carrying amounts			
At 30 June and 1 July 2019	104	47	151
At 30 June 2020	75	34	109

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 \$122k as at 30 June 2020 (2019: \$nil). This all relates to the NotifyUs tool, some of which was included in Work in Progress as at 30 June 2020.

Work in progress

The capital work in progress figure for 2020 is \$82k (2019: \$nil). Most of these costs are associated with the development of the new NotifyUs tool to report privacy breaches.

Note 11: Payables

Accounting policy

Creditors and other payables are recorded at the amount payable.

Breakdown of payables

	Actual 2020 \$000	Actual 2019 \$000
Payables under exchange transactions		
Creditors	208	135
Accrued expenses	112	68
Lease incentive	18	20
Total payables under exchange transactions	338	223
Payables under non-exchange transactions		
Other payables	-	46
Total payables under non-exchange transactions	-	46
Total creditors and other payables	338	269

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 12: Non-current liabilities

	Actual 2020 \$000	Actual 2019 \$000
Lease incentive	29	12
Total non-current liabilities	29	12

Lease incentive for the Wellington office for the period 23 February 2015 to 22 February 2021 (6-year lease).

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

Note 13: Employee entitlements

Accounting policy

Employee entitlements that the Privacy Commissioner expects to be settled within 12 months of balance date are measured at undiscounted nominal values based on accrued entitlements at current rates of pay.

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

The Privacy Commissioner recognises a liability for sick leave to the extent that compensated absences in the coming year are expected to be greater than the sick leave entitlements earned in the coming year. The amount is calculated based on the unused sick leave entitlement that can be carried forward at balance date, to the extent the Privacy Commissioner anticipates it will be used by staff to cover those future absences.

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.

Breakdown of employee entitlements:

	Actual 2020 \$000	Actual 2019 \$000
Current employee entitlements are represented by:		
Accrued salaries and wages	86	64
Annual leave	232	156
Total current portion	317	220
Current	317	220
Non-current	-	-
Total employee entitlements	317	220

Note 14: Contingencies

Quantifiable contingent liabilities are as follows:

The Privacy Commissioner is subject to a “Make Good” clause in its lease contracts for the Auckland and Wellington offices. This clause, if invoked, would require the Privacy Commissioner to remove all leasehold improvements and leave the premises in a state not dissimilar to that at the time of moving into the premises.

The lease on the Wellington office will expire in February 2021. At balance date, a decision had not yet been made on whether to continue to lease the current premises. The likelihood of the clause being invoked is unknown, as is the cost to fulfil the clause if invoked.

Other than as stated above, there are no known contingencies existing at balance date (2019: \$nil).

Note 15: 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 2020	Actual 2019
Total salaries and other short-term employee benefits (\$000)	926	1,050
Full-time equivalent members	4.3	5

Key management personnel include all Senior Managers and the Privacy Commissioner who together comprise the Senior Leadership Team (SLT). Two members of the SLT left during the year, with one being replaced part way through the year and the other vacancy still in place at year-end.

Note 16: Post balance date events

There are no 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 17: Financial instruments

Financial instrument categories

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

	2020 \$000	2019 \$000
FINANCIAL ASSETS		
Financial assets measured at amortised cost		
Cash and cash equivalents	1,093	840
Receivables (excluding prepayments and taxes receivable)	136	49
Total loans and receivables	1,229	889
FINANCIAL LIABILITIES		
Financial liabilities at amortised cost		
Payables (excluding income in advance, taxes payable, grants received subject to conditions and lease incentive)	320	203
Total financial liabilities at amortised cost	320	203

Note 18: COVID-19 Financial Impact Assessment

The Privacy Commissioner made the following assessments on the financial implications of COVID-19.

Revenue

- there was no impact on Crown Revenue.

Expenditure

- staff development costs were lower than budget partly due to the impact of COVID-19;
- the accumulated leave balance was higher than budget as staff holiday plans were impacted by COVID-19;
- travel costs were lower than budget as a result of the COVID-19 travel restrictions;
- there were several un-budgeted IT related costs during the lockdown to support staff working from home.

Others and significant assumptions

- there are no provisions made for COVID-19 impact within the Privacy Commissioner's balance sheet including debtors. Total short-term debtors (excluding GST receivable) at year-end was \$136k. 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 forms the regulatory side of the Office's functions. The team investigates complaints from the public about interferences with individuals' privacy.

An interference with privacy occurs when an agency has breached a privacy principle and caused the complainant harm, such as negative physical, emotional or financial effects. However, a complainant does not have to demonstrate harm in cases involving access or correction of information.

During an investigation we determine:

- whether the Privacy Act covers the issue
- whether the respondent agency is responsible
- the level of harm that the breach caused.

We can compel agencies to produce documents and meet with complainants. We cannot compel complainants or respondents to accept settlement terms and we cannot award damages. However, our view is an important indication of whether there's been an interference with privacy.

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

When there has been an interference with privacy and the two parties cannot settle the case, 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. He can then choose to bring the case before the Tribunal.

Policy

Our Policy team provides advice to a range of organisations on the privacy risks of various initiatives. We also offer advice to help organisations mitigate privacy risks.

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

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

We 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 matching

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

Information matching raises several privacy issues, such as the potential to disclose incorrect date information or the potential to 'automate away' human judgement. For this reason, the Privacy Act regulates information matching in the public sector.

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

Communications and outreach

Our Communications team works to raise privacy awareness. We work through a significant number of channels, producing material such as:

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

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

We respond to enquiries from journalists in traditional media and the public on social media.

Appendix B

Information matching 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, s 246 and Tax Administration Act 1994, Schedule 7 Part C subpart 2 cl 41 **Compliance**

1. IR/ACC Compensation and Levies

To confirm income amounts for compensation calculations.

Inland Revenue (IR) disclosure to ACC: For self-employed people, IR provides ACC with the full name, contact details, date of birth, IR number and earnings information. For employers, IR provides ACC with the name, address, IR number, and total employee earnings.



Accident Compensation Act 2001, s 280 **Compliance**

2. Corrections/ACC Prisoners

To ensure that prisoners do not continue to receive earnings-related accident compensation payments.

Corrections disclosure to ACC: Corrections provides ACC with the surname, given names, date of birth, gender, date received in prison and any aliases of all people newly admitted to prison.



Accident Compensation Act 2001, s 281 **Compliance**

3. ACC/MSD Benefit Eligibility

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

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

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

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



4. BDM (Births)/IR Newborns Tax Number

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

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.

**5. BDM (Births)/MoH NHI and Mortality Register**

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

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.

**6. BDM/MSD Identity Verification**

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

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

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.

**7. BDM (Deaths)/GSF Eligibility**

To identify members or beneficiaries of the Government Superannuation Fund (GSF) who have died.

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.

**8. BDM (Deaths)/INZ Deceased Temporary Visa Holders**

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

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

**9. BDM (Deaths)/IR Deceased Taxpayers**

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

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.

**10. BDM (Deaths)/MoH NHI and Mortality Register**

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

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

**11. BDM (Deaths)/MSD Deceased Persons**

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





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.

**12. BDM (Deaths)/NPF Eligibility**

To identify members or beneficiaries of the National Provident Fund (NPF) who have died.

BDM disclosure to NPF: BDM provides information from the NZ Deaths Register covering the 12 weeks prior to the extraction date. The information includes full name at birth, full name at death, gender, date of birth, date of death, place of birth, and number of years lived in New Zealand (if not born in New Zealand).



<p>13. 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 NZ 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>14. 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>15. 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. The details displayed include full name, gender, date of birth, place of birth and parents' full names.</p>	
<p>16. BDM/DIA(Passports) Passport Eligibility</p>	
<p>To verify, by comparing details with the Births, Deaths and Marriages registers, whether a person is eligible for a passport, and to detect fraudulent applications.</p>	
<p>BDM disclosure to Passports (DIA): Possible matches from the Births, Deaths and Marriages (relationships) databases are displayed to Passports staff as they process each application. The details displayed include full name, gender and date of birth.</p>	
<p>17. BDM/MSD Overseas Born Name Change</p>	
<p>To verify a client's eligibility or continuing eligibility for a benefit where a client has legally changed their name in New Zealand and not informed MSD. The programme is also used to identify debtors and suspected benefit fraud.</p>	
<p>BDM disclosure to MSD: BDM provides name change records from January 2009 to the extraction date. The name change details include the full name at birth, former full name, new full name, date of birth, residential address, and country of birth.</p>	

18. DIA (Citizenship)/BDM Citizenship by Birth Processing

To enable the Registrar-General to determine the citizenship-by-birth status of a person born in New Zealand on or after 1 January 2006, for the purpose of recording the person's citizenship status on his or her birth registration entry.

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.

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.



19. DIA(Citizenship)/DIA(Passports) Passport Eligibility

To verify a person's eligibility to hold a New Zealand passport from Citizenship database information.

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.



20. Citizenship/INZ Entitlement to Reside

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

Citizenship 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.

21. Corrections/MSD Prisoners

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

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.



22. Corrections/INZ Prisoners

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.

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

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



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

23. Customs/IR Student Loan Alerts

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

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

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



24. Customs/IR Student Loan Interest

To detect student loan borrowers who leave for, or return from, overseas so that IR can administer the student loan scheme and its interest-free conditions.

IR disclosure to Customs: IR provides Customs with the full name, date of birth, and IR number for student loan borrowers who have a loan of more than \$20.

Customs disclosure to IR: For possible matches to borrowers, Customs provides the full name, date of birth, IR number and date, time and direction of travel.

Customs and Excise Act 2018, s 307 **Compliance**

25. Customs/IR Child Support Alerts

To identify parents in serious default of their child support liabilities who leave for or return from overseas so that IR can take steps to recover the outstanding debt.

IR disclosure to Customs: IR provides Customs with the full name, date of birth, and IR number of parents in serious default of their child support liabilities.

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



Customs and Excise Act 2018, s 309 **Compliance**

26. Customs/MSD Periods of Residence

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

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



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

27. Customs/Justice Fines Defaulters Alerts

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

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

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



Education Act 1989, s 226A and s 235F	Compliance
<p>28. 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>	
	
Education Act 1989, s 307D	Compliance
<p>29. 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 Act 1989, s 360	Compliance
<p>30. MoE/Teaching Council Teacher Registration</p> <p>To ensure teachers are correctly registered (Education Council) and paid correctly (Ministry of Education).</p> <p>MoE disclosure to Education 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>Education Council disclosure to MoE: The Education Council provides full name, date of birth, gender, address, registration number, registration expiry date, registration classification and MoE employee number (if confirmed).</p>	
	
Electoral Act 1993, s 263A	Compliance
<p>31. 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>	
	

32. DIA (Citizenship)/EC Unenrolled Voters

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

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

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

To compare passport records with the electoral roll to:

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

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

**34. MSD/EC Unenrolled Voters**

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

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

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

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

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

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

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

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

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

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

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



Electronic Identity Verification Act 2012, s 39**Compliance****37. DIA Identity Verification Service (IVS)**

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

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

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

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

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

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

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

**Immigration Act 2009, s 300****Compliance****38. INZ/MoH Publically Funded Health Eligibility**

To enable the Ministry of Health to determine an individual's:

- eligibility for access to publically funded health and disability support services; or
- liability to pay for publically funded health and disability support services received.

MoH disclosure to INZ: MoH sends names, date of birth and NHI number to INZ for matching.

INZ disclosure to MoH: INZ provides names, gender, birth date, nationality, visa or permit type and start and expiry dates, and dates the person entered or left New Zealand. INZ may also disclose details of a parent or guardian of a young person.

**Motor Vehicle Sales Act 2003, s 122 and s 123****Compliance****39. NZTA/MBIE Motor Vehicle Traders Sellers**

To identify people who have sold more than six motor vehicles in a 12-month period and are not registered as motor vehicle traders.

Waka Kotahi disclosure to MBIE: Waka Kotahi 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.

MBIE disclosure to Waka Kotahi: MBIE provides Waka Kotahi 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.

**Social Security Act 2018, Schedule 6, cl 13****Compliance****40. MSD/Justice Fines Defaulters Tracing**

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

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

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

**Social Security Act 2018, Schedule 6, cl 15****Compliance****41. Justice/MSD Warrants to Arrest**

To enable MSD to suspend or reduce the benefits of people who have an outstanding warrant to arrest for criminal proceedings.

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.



Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Australia) Order 2017 **Compliance**

42. Australia (Centrelink)/MSD Change in Circumstances

For MSD and Centrelink (the Australian Government agency administering social welfare payments) to exchange benefit and pension applications, and changes of client information.

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.

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.



Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Malta) Order 2013 **Compliance**

43. Malta/MSD Social Welfare Reciprocity

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

Malta disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information and Maltese Identity Card and Social Security numbers.

MSD disclosure to Malta: includes full name, date of birth, marital status, address, entitlement information and MSD client number.



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

44. Netherlands/MSD Change in Circumstances

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

MSD disclosure to Netherlands: MSD forwards the appropriate application forms to the Netherlands Sociale Verzekeringsbank (SVB). The forms include details such as the full names, dates of birth, addresses and MSD client number.

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



45. Netherlands/MSD General Adjustment

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

MSD disclosure to Netherlands: For MSD clients in receipt of both New Zealand and Netherlands pensions, MSD provides the Netherlands Sociale Verzekeringsbank (SVB) with the changed superannuation payment information, the MSD client reference number and the Netherlands unique identifier.

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



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

46. United Kingdom/MSD Social Welfare Reciprocity

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

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

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



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

47. IR/Justice Fines Defaulters Tracing

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

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

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



Online transfer approvals

The Privacy Act 1993 Schedule 4 Rule 3 prohibits the transfer of information by online computer connections except with the Commissioner's approval. We grant approvals subject to conditions designed to ensure that agencies put in place appropriate safeguards to protect the data.

The practice of the Office has usually involved granting first-time approvals for 12 months.

Based on evidence of safe operation in that first period, and verified by a satisfactory audit report, subsequent approvals are typically issued for a three-year term.

This control has been omitted from the Privacy Act 2020. To compensate for the loss of this control the annual reporting requirements are being extended to cover the primary threats such as failure to use current versions of software.

User Agency Programme(s) name(s) Approval Date	Reason	Grounds
Department of Internal Affairs		
1. BDM/DIA(Citizenship) Citizenship Application Processing 2. BDM/DIA(Passports) Passport Eligibility 3. Citizenship/BDM Citizenship by Birth Processing 4. Citizenship/DIA(Passports) Passport Eligibility 17 February 2020	Efficiency – transfer is within agency	Satisfactory audit result
Electoral Commission		
INZ/EC Unqualified Voters 7 November 2019	Efficiency and data quality	Timely delivery of data
Inland Revenue		
BDM (Deaths)/IRD Deceased Taxpayers 26 September 2019	Efficiency and security	Timely delivery of data
Customs/IR Child Support Alerts Customs/IR Student Loans Alerts 20 July 2020	Efficiency and security (SEEMail)	Satisfactory audit result
Customs/IR Child Support Person of Interest Customs/IR Child Support Alerts Customs/IR Student Loan Person of Interest Customs/IR Student Loan Alerts 2 April 2020	Efficiency (API)	Timely delivery of data
Ministry of Health		
BDM (Deaths)/MoH NHI & Mortality Register 28 January 2020	Efficiency and security	Timely delivery of data

Ministry of Social Development		
Educational Institutions/MSD Loans and Allowances [VoS] 26 October 2019	Efficiency and security (email)	Timely delivery of data
Justice/MSD Warrant to Arrest 20 July 2020	Efficiency and security	Timely delivery of data
Educational Institutions/MSD Student Loans and Allowances (Verification of Study [VoS]) MoE/MSD Results of Study Match [RoS] 5 August 2020	Efficiency (website)	Timely delivery of data
Australia (Centrelink)/MSD Change in Circumstances 13 December 2019	Efficiency and security	Satisfactory audit result
MBIE		
NZTA/Registered Motor Vehicle Traders – Motor Vehicle Sellers 8 July 2019	Efficiency and security	Satisfactory audit result
Teaching Council of Aotearoa New Zealand		
MoE/Teaching Council Teacher Registration Match 20 July 2020	Efficiency and security	Timely delivery of data

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 2020

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 45 to 66, that comprise the statement of financial position as at 30 June 2020, 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 7 to 8 and 35 to 44.

In our opinion:

- the financial statements of the Privacy Commissioner on pages 45 to 66:
 - present fairly, in all material respects:
 - its financial position as at 30 June 2020; 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 Public Benefit Entity Standards Reduced Disclosure Regime; and
- the performance information on pages 7 to 8 and 35 to 44:
 - presents fairly, in all material respects, the Privacy Commissioner's performance for the year ended 30 June 2020, 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.
 - complies with generally accepted accounting practice in New Zealand.

Our audit was completed on 04 December 2020. This is the date at which our opinion is expressed.

The basis for our opinion is explained below, and we draw attention to the impact of Covid-19 on the Privacy Commissioner. 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.

Emphasis of matter – Impact of Covid-19

Without modifying our opinion, we draw attention to the disclosures about the impact of Covid-19 on the Privacy Commissioner as set out in note 18 to the financial statements and page 35 of the performance information.

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 they determine is necessary to enable them 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 1 to 6, 9 to 34 and 67 to 80, 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

© 2020 The Privacy Commissioner
ISSN 1179-9838 (Print)
ISSN 1179-9846 (Online)