Privacy Commissioner
Te Mana Matapono Matatapu

Office of the Privacy Commissioner
PO Box 10094, The Terrace, Wellington 6143
Level 11, 215 Lambton Quay
Wellington, New Zealand
P +64 4 474 7590 F +64 4 474 7595
E enquiries@privacy.org.nz
0800 803 909 Enquiries
privacy.org.nz

2 February 2024

Hon Paul Goldsmith
Minister of Justice
Parliament Buildings
WELLINGTON

Dear Minister

QUARTERLY REPORT OF THE PRIVACY COMMISSIONER FOR THE PERIOD 1 OCTOBER 2023 TO 31 DECEMBER 2023

Highlights

We have been experiencing high operational volumes and pressure on our front-line services. In the 2022/23 financial year, the number of privacy complaints increased by 79 percent compared to the prior year and serious privacy breaches by 59 percent. These increases are caused through many New Zealand agencies (both public and private) having low privacy capability and compliance, leading to significant privacy related harms. Lack of capability also means that breaches are under-reported, meaning that the real level of privacy harm is likely much greater than recorded. Our assessment of critical operational risks has regulatory failure as our most critical risk, where New Zealanders lose confidence that their privacy is being protected.

Our current level of funding hampers our ability to respond effectively to the increasing volume of privacy breaches and complaints or fully deliver on our statutory responsibilities in a way that meets the expectations of citizens and agencies. We are reporting a deficit of $152,000 for the 6 months ending 31 December 2023 and forecasting a deficit of $348,000 for the year to June 2024. The deficit is currently being met from cash reserves, but that cannot continue for much longer. The fiscal savings review will further add to this challenge.

We are continuing to execute our organisational strategy of ensuring that privacy is a core focus for agencies. This includes setting clear expectations for agencies. In November, we announced that we will release an exposure draft of a Code of Practice under the Privacy Act 2020 to test tighter controls on how agencies collect, analyse and use biometric information when using automated biometric processing. In December, we completed an engagement process with professionals who work with children (such as teachers and doctors) and children advocacy agencies, and this has demonstrated a strong appetite and need for further work into children's privacy. In December we also established a Digital Regulators Forum with key government agencies to encourage collaboration and promote more coherent approaches to digital regulatory matters.

The state of privacy in New Zealand

The Privacy Act places obligations to protect personal information on almost all agencies operating in New Zealand – across the public, private and not-for-profit sectors. By doing so, the Privacy Act enables New Zealanders to have trust in the companies and government services that they use every day.

Appendix A outlines some of our key operational volumes. The volume of privacy harms being experienced is increasing, placing pressure on our front-line services. In the 2022/23 financial year, the number of privacy complaints increased by 79 percent compared to the prior year. The volume of serious privacy breaches increased by 59 percent over the same period. Our operational volumes in the 2023/24 year to date have continued at very high levels. It is difficult to compare privacy breaches and the harms they cause due to each breach being different in its cause and impact. For example, the majority of privacy breaches affect a relatively small number of individuals, with a small number of breaches affecting many thousands or millions of people.

Our experience is that many agencies have low privacy capability and compliance. Very few agencies are meeting all of their privacy requirements under the Privacy Act, although some have robust processes for certain requirements (such as providing individuals with access to their own information). It is for this reason that we have focused our organisational strategy on making privacy a core focus.

A primary driver behind low privacy capability and compliance is the lack of accountability and consequences for managing personal information poorly. Many agencies we investigate are aware that the Privacy Act has no meaningful financial penalties and that we have relatively limited compliance powers that we can use. Consequently these agencies are not incentivised to consider privacy, including cyber-security risks, in the same way they consider other requirements, such as complying with financial reporting standards or health and safety.

From a Government information sharing perspective, legislation is not the primary barrier preventing public sector agencies from sharing personal information where necessary for public services. Capability and organisational culture and risk averseness are often the root cause. We are working with the Government Chief Privacy Officer on ways to build the public sector's information sharing capability. We need greater emphasis on the ability of operational staff to understand and use the wide-ranging information sharing mechanisms available, including those available under the Privacy Act. Using these approaches ensures that public trust and social license is maintained.

Our current level of funding hampers out ability to effectively address the significant regulatory failure occurring across the public and private sectors under the Privacy Act. For example, we are not resourced to investigate the complex cyber attacks that are increasingly common, despite the Privacy Act being the only regulation that requires agencies to take reasonable steps protect the information they hold against security breaches.

Activities of our Office

Compliance and enforcement

Our Compliance and Enforcement team responds to privacy breach notifications and undertakes compliance investigations. This team also supports agencies with identified systemic issues to improve privacy practice and culture. For example, during this reporting period we engaged with Oranga Tamariki – Ministry of Children and Te Whatu Ora – Health New Zealand about our systemic concerns about their privacy practices and systems.

A key focus for us over the past year has been to strengthen our Compliance and Enforcement team. Good progress has been made in this area, through expanding the size of the team from three to six and improving their policies and procedures to increase both the quality and quantity of compliance activities undertaken.

In December 2022, as part of a joint inquiry with the Independent Police Conduct Authority, we issued a Compliance Notice with 14 requirements for improving New Zealand Police practices for the taking and retention of photographs and fingerprints of children, young people and adults. The requirements were due to be completed by Police by 31 December 2023 and we are assessing the progress made towards this deadline. Police have requested an extension to two requirements and this request to vary the Compliance Notice completion date is currently being assessed.

In May 2023 we initiated a joint compliance investigation with the Office of the Australian Information Commissioner into the Latitude Financial (operating in New Zealand as Gem Finance) data breach that exposed the personal information of millions of Australians and New Zealanders. To date this is New Zealand's largest data breach involving over 1 million New Zealanders. The focus of the compliance investigation is on Latitude's information retention policies and practices, and the security settings of the systems that held the information. Initial indications suggest that Latitude was retaining information for longer than it needed to, raising concerns under Information Privacy Principle 9 of the Privacy Act. The compliance investigation continues to progress well both in terms of our engagements with Latitude Financial and with working with our Australian counterparts. The timeframe for resolving the matter will become clearer as we continue our enquiries with Latitude and we are mindful of aligning timing with our Australian counterparts.

Investigations and dispute resolution

Over the past six months we have received a large number of privacy complaints from individuals affected by the Latitude Financial data breach. During this reporting period the number of privacy complaints from current or past customers of Latitude Financial began to reduce. We have deliberately phased the compliance and individual complaint investigations to happen consecutively as the information we gather through the joint compliance investigation will help inform consideration of individual complaints and reduce the need for duplicate processes. This approach also allows for the possibility and the pros and cons of New Zealand complainants joining a potential representative (class) action through our Australian counterparts and/or the Australian Courts to be considered, should such action proceed.

Our response to high numbers of other privacy complaints has been to focus on early resolution. Our fast resolve process is focused on ensuring that full complaint investigations only occur when the complaint is valid and the individual cannot resolve the issue with the agency themselves. During this reporting period 159 complaints were addressed through the fast resolve process, with a resolution rate of nearly 84 percent.

Even with the fast resolve process the timeliness of our complaints process remains under pressure. Our timeliness target is to have 85 percent of complaints closed within six months, and we are currently at 80 percent. People are waiting approximately 150 days before a complaint is assigned for action. The timeliness of our complaints processes is an area that privacy complainants are likely to complain to us about and has led to inappropriate and abusive behaviour. We manage this behaviour in line with our policy on Managing Unreasonable Complainant Conduct and have developed a detailed Physical Security Threat Response Plan. We have also developed a decision guide to help the public and agencies better understand our complaint investigation processes.

We aim to have 50 percent of our fully investigated privacy complaints resolved through settlement between the parties. In the past six months we have achieved a settlement rate of 57 percent and these have involved cash settlements totalling $243,500. The largest number of privacy complaints are from individuals about issues they have in exercising their right to access the personal information that agencies hold about them, followed by complaints about the security and disclosure of personal information. Our alternative dispute resolution approach functions to take the pressure off the Human Rights Review Tribunal where waiting times for consideration are currently very long.

Capability and guidance

This reporting period we established a new Capability and Guidance team to provide more support to agencies on how to meet the expectations in the Privacy Act. The key new responsibility of this team is to implement a programme of work to overhaul and streamline our guidance to agencies (known as *Poupou Matatapu – Doing Privacy Well*) and improving our regulatory stewardship of our guidance material.

The Capability and Guidance team has also inherited some responsibilities from the Policy team relating to Government information sharing. During this reporting period this included providing support on Privacy Act Approved Information Sharing Agreements through:

- Reviewing additional Operational Procedures for the Gang Harm Intelligence Centre
- Further supporting the development of a Veterans Affairs Information Sharing Agreement as it progresses
- Reviewing Operating Procedures provided by the Department of Internal Affairs for the Identity Services Approved Information Sharing Agreement
- Providing input into the Department of Internal Affairs agreement relating to death information, including reviewing additional Operational Protocols.

Other work undertaken by the Capability and Guidance team included:

- Responding to consultation on revised Naming Policies under the Health Practitioners Competence Assurance Act

- Consulting with the New Zealand Customs Service on an Information Sharing Agreement under the Customs and Excise Act
- Working with the Department of Internal Affairs regarding information sharing under the Passports Act.

Policy and international

In November 2023 we announced that we would be consulting on new draft rules (a "Code of Practice" under the Privacy Act) specifically for biometrics. Work began in this quarter to confirm the policy underpinnings of this Code and to start drafting the exposure draft. If such a Code is put in place, it would place tighter controls on how the Privacy Act applies to agencies using biometric technology to collect, analyse and use biometric information. There is strong interest in this work, with media coverage including TVNZ Breakfast, Radio New Zealand, Newstalk ZB and Mediaworks.

Throughout 2023 we undertook substantial work on Artificial Intelligence (AI) and privacy. This included issuing our expectations for agencies using AI tools (May 2023) and explaining how the Information Privacy Principles apply to AI (September 2023). We are continuing our work on Artificial Intelligence, including through being involved in wider Government processes.

During this reporting period we established a Digital Regulators Forum with those government agencies that have a role in regulating digital regulatory matters[1] such as AI. The Forum will be exploring what work could be jointly undertaken with these agencies.

We completed an engagement process on children's privacy, by seeking information from professionals who work with children (such as teachers and doctors), and non-governmental organisations who advocate for children and young people. The 113 submissions we received have made it clear that there is a strong appetite and need for further work in this area, and we are accordingly working through our next steps for this work.

During this reporting period we made the submissions on the

- Ram Raid Offending and Related Measures Amendment Bill
- Electoral (Lowering Voting Age for Local Elections and Polls) Legislation Bill

In early December the Asia Pacific Privacy Authorities (APPA) Forum met in Sydney, providing an opportunity for representatives from country and state privacy authorities to share information on the latest privacy developments in their jurisdictions. The Privacy Commissioner spoke on AI, our *Poupou Matatapu – Doing Privacy Well* initiative, and biometrics and privacy. A particular highlight was being able to leverage these events to build relationships with our Australian counterparts in person, including the team leading the investigation into the Latitude Financial breach.

[1] The Department of Internal Affairs, Ministry of Business, Innovation and Employment, StatsNZ and the Commerce Commission.

Communication and engagement

Immediately prior to the APPA Forum in Sydney, the annual Australia New Zealand summit of the International Association of Privacy Professionals was held. The Privacy Commissioner gave a keynote speech at this summit, focusing on the work of our Office over the last 12 months, proposals for amendments to the Privacy Act to made it fit-for-purpose in the digital age, AI, and the need for governance bodies to take privacy seriously.

The media represents a critical communications channel for the Privacy Commissioner to raise awareness of privacy issues and provide real-time advice and guidance to private sector in particular. During this period we provided media comment on multiple privacy breaches, including for Te Whatu Ora – Health New Zealand, Auckland City Council (Watercare) and ACC. Major privacy issues that were prevalent in the media included facial recognition technology, genetic testing websites and photography on flights.

Two of our case notes (anonymous summaries of privacy breach complaints) were picked up by the media. One involved an incorrect template that cost an organisation $15,000 and the other about a woman's photo being displayed publicly in a reception area.

We have announced the theme for Privacy Week 2024 as 'Busting Privacy Myths' and have begun arranging potential presenters for webinars related to this theme. Privacy Week 2024 will run from 13-17 May 2024.

The management of organisational risk

We maintain an ongoing assessment of the critical operational risks that we face us and our mitigations. Our Senior Leadership Team and Legislative Compliance Working Group monitor these risks regularly throughout the year.

Our most critical risk continues to be regulatory failure, where New Zealanders lose confidence that their privacy is being protected, likely due to a series of high-profile serious privacy breaches. Our efforts to address this risk include implementing *Poupou Matatapu – Doing Privacy Well*, a programme of clear guidance to agencies that identifies how to meet the key requirements of the Privacy Act. As previously reported, we do not believe that we have sufficient funding to respond effectively to the increased volume in breaches and complaints or fully deliver on our statutory responsibilities in a way that meets the expectations of citizens and agencies. The current fiscal savings review will further add to this challenge and as an Office we are currently assessing how best to address this whilst not impacting on our ability to deliver core services.

Other areas of high risk remain consistent and include the possible failure to target our activities for maximum impact, meeting our statutory responsibility to take account of cultural perspectives on privacy and failure to attract and retain people. Mitigations have been identified for these areas.

Financial report

We are reporting a deficit of $152,000 for the six months ending 31 December 2023. This is in excess of the deficit budgeted of $21,000 as a result of changes in staffing and increased operating costs particularly in computer maintenance and network costs. We are currently forecasting a deficit of $348,000 for the year to June 2024. The Office will be utilising cash reserves to fund this deficit for the current financial year. Further details of financial information and performance against the Statement of Performance Expectations are included as appendices to this report.

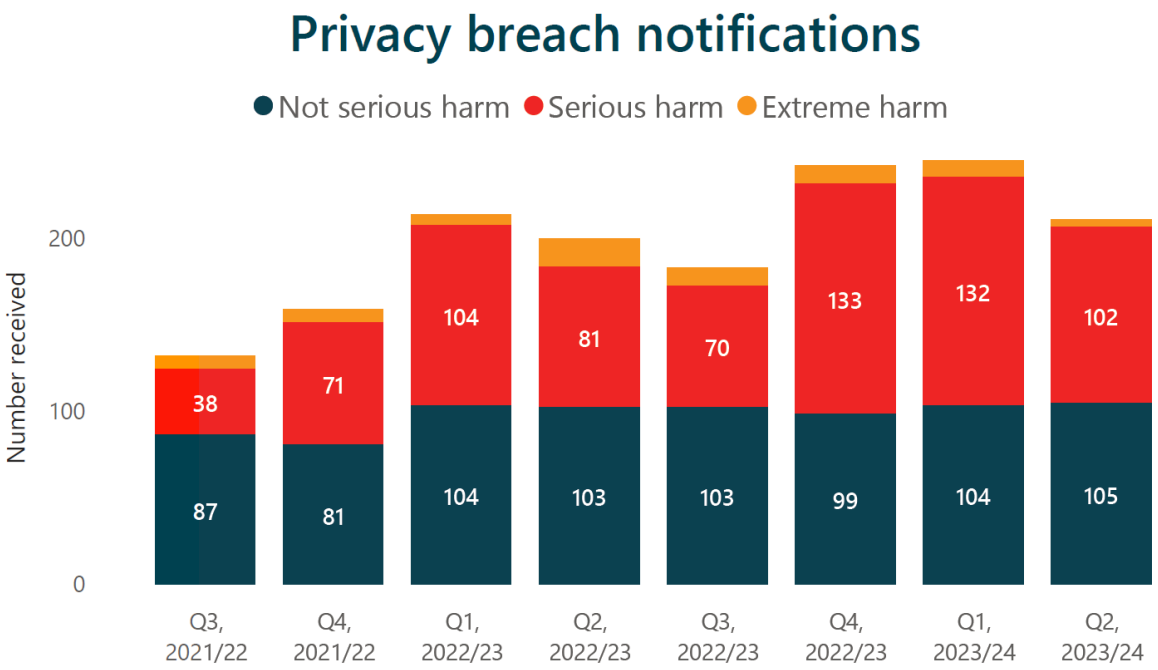
Our external auditors, Deloitte expressed a clear audit report on the 31 October 2023 at the completion of the audit process for the year ended 30 June 2023. There were no significant matters arising from the audit. Some minor process improvements were recommended by our auditors, and these have been implemented.

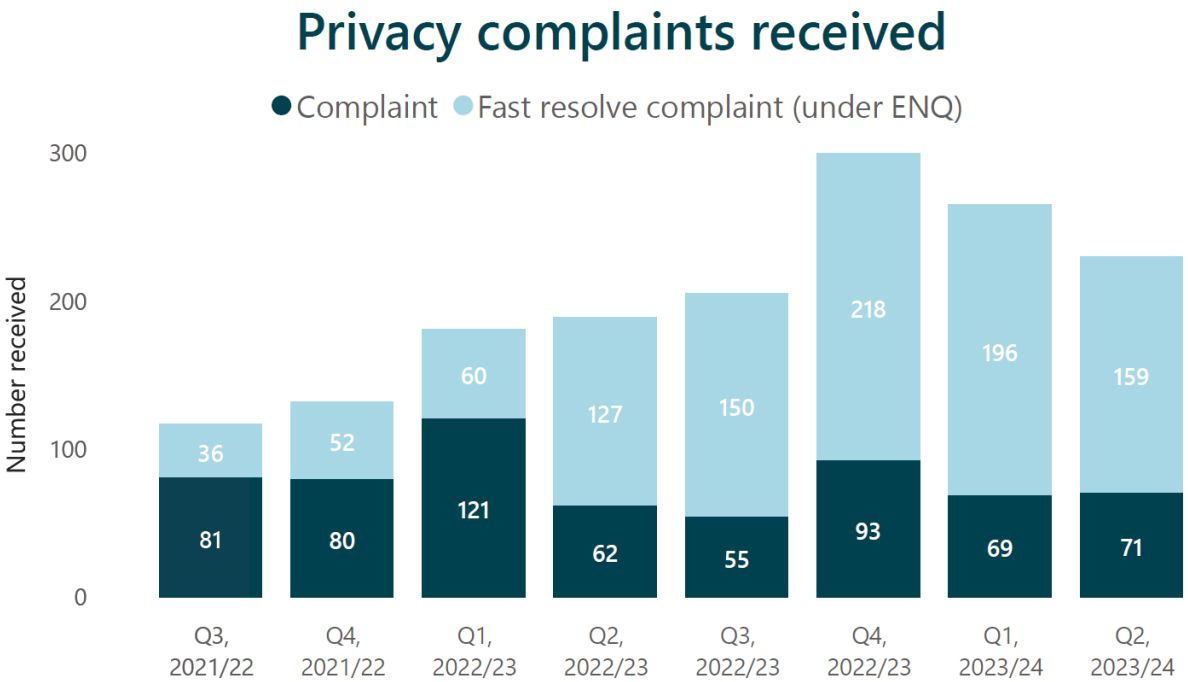
Yours sincerely

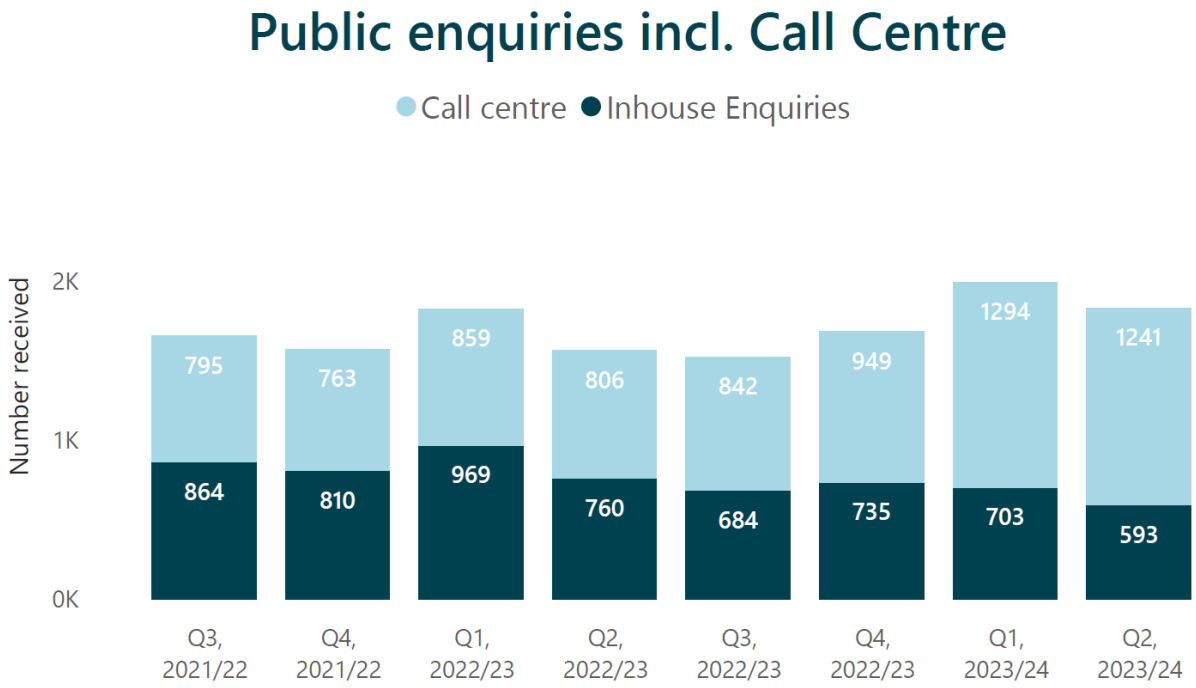
Michael Webster
Privacy Commissioner

Encl:	Appendix A:	Key operational volumes
	Appendix B:	Financials for period ending 31 December 2023
	Appendix C:	Performance against Statement of Performance Expectations - Year to Date
	Appendix D:	Q1 KPI Trend Report – December 2023

Appendix A: Key operational volumes






Public enquiries incl. Call Centre
Call centre
Inhouse Enquiries
Number received
2K
1K
0K
795
763
859
806
842
949
1294
1241
864
810
969
760
684
735
703
593
Q3, 2021/22
Q4, 2021/22
Q1, 2022/23
Q2, 2022/23
Q3, 2022/23
Q4, 2022/23
Q1, 2023/24
Q2, 2023/24