

5 November 2024

Hon Paul Goldsmith
Minister of Justice
Parliament Buildings
WELLINGTON

Dear Minister

QUARTERLY REPORT OF THE PRIVACY COMMISSIONER FOR THE PERIOD 1 JULY 2024 TO 30 SEPTEMBER 2024

Highlights

We completed our first Annual Report under the Statement of Intent 2024-2027, which showed that 2023/24 was a big year for privacy. The number of privacy complaints we received from individuals increased by 15% and privacy breach notifications from by 3% (in comparison to 2022/23).

This quarter has seen our key operational volumes increase again, with serious harm privacy notifications increasing by 27% and privacy complaints increasing by 15% (in comparison to the April to June 2024 period). More information on our key operational volumes is available in Appendix A.

One significant achievement for us this quarter was issuing a free online toolkit designed to help agencies understand and meet their privacy responsibilities: Poupou Matatapu – Doing Privacy Well. This toolkit is designed to assist privacy management and help build data quality, customer and stakeholder trust and decision-making processes. Poupou Matatapu is the core guidance that we refer agencies to as we seek to build privacy understanding across New Zealand.

In September, Foodstuffs North Island announced that their facial recognition system trial across 25 New World and PAK'nSAVE supermarkets was successful in avoiding approximately 130 safety incidents. We are currently awaiting the results of the independent evaluation that Foodstuffs commissioned so that this will inform our Inquiry into the trial. We expect to complete our Inquiry this calendar year.

We assessed the submissions we received on the exposure draft Code of Practice for biometric technologies. We analysed 250 submissions received in response to our April exposure draft and undertook targeted meetings with key stakeholders. Informed by public submissions and stakeholder views, we are preparing advice for the Privacy Commissioner to formally consider whether a revised draft Code should be publicly released for consultation.

How the Privacy Act 2020 can help address retail crime

Retailers are seeking more guidance from us about how the Privacy Act can address retail crime, especially through information sharing and implementing new technologies. In September, the Privacy Commissioner invited the Chief Executive of Retail NZ, Carolyn Young, to a meeting to discuss these issues

The principles-based nature of the Privacy Act means that agencies can develop information handling practices that fit with their lawful purposes and business needs. The Privacy Act also contains exceptions that allow personal information disclosures for the purposes of safety and maintenance of the law (including crime prevention).

One area we will be considering for future guidance is where businesses are working together or co-ordinating on a common objective such as responses to increasing levels and types of retail crime. The flexible nature of the Privacy Act means there is scope for retailers to develop ways to share information when to do so would clearly contribute to a common purpose, such as protecting a common retail space from aggressive and unlawful behaviours. The key aspect for retailers will be to put in place clear policies and understandings that reflect what personal information will be shared with the other proximate retail businesses and for what purposes.

We are working Retail NZ as we progress with this issue and will leverage their communications with their members. This will include sharing information on our existing guidance such as how to implement CCTV and Poupou Matatapu – Doing Privacy Well.

Activities of our Office

Policy

We continued supporting the Ministry of Justice with the progression of the Privacy Amendment Bill and the Statutes Amendment Bill (with its minor amendments to the Privacy Act) as they progressed through to their respective Select Committees for consideration.

Our work in reviewing policy initiatives substantially increased this quarter as the Government's legislative programme expands. These initiatives included:

- establishing an offence for stalking
- reforms to the Holidays Act 2003
- amendments to the Arms Act 1983
- the Budapest Convention and Related Matters Legislation Amendment Bill, which will align New Zealand legislation with the Council of Europe Convention on Cybercrime
- legislative amendments relating to foreign interference
- amending regulations made under the Corrections Act 2004
- amending regulations made under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009
- amendments to the Child Sex Offender Register
- reviewing court procedures in sexual violence cases, including name suppression
- working with the Crown Response Unit following the report of the Royal Commission on Abuse in Care
- the use of attendance data and National Student Numbers by the Ministry of Education.

We also made four submissions to Select Committee relating to Government legislation:

- Contracts of Insurance Bill (with a focus on issues of privacy and genetic testing)
- Taxation (Annual Rates for 2024-25, Emergency Response and Remedial Measures) Bill
- Consumer and Product Data Bill
- Transport (drug driving) Amendment Bill.

Capability and guidance

One of our statutory roles is to comment on the Government information sharing proposals made under the Privacy Act known as Approved Information Sharing Agreements (AISAs). AISAs authorise agencies to share personal information to facilitate the provision of public services and fourteen have been established since 2011.

During this quarter, our Capability and Guidance team reviewed and provided feedback on the operational protocols of multiple AISAs led by the Department of Internal Affairs (DIA). DIA houses a number of different regulators operating under different legislative structures. The AISAs variously enable the internal sharing of personal information between DIA based regulators, information about individuals using DIA's services and for notifying a wide range of agencies when individuals have deceased.

We have also initiated a review of the Gang Intelligence Centre Approved Information Sharing Agreement that was established in 2019.

Other work undertaken during this quarter includes:

- responding to statutory consultations on multiple international information sharing agreements, including under the Policing Act 2008 and Biosecurity Act 1993.
- assisting agencies on large information architecture-related projects they are undertaking, including Health New Zealand and the Ministry of Education.
- preparing guidance to help build understanding on the operation of the Privacy Act, including on the operation of section 11 (e.g. for cloud storage providers), the rental sector and Health Information Privacy Code.

Communication and engagement

During this quarter we updated our website's homepage at no cost using only internal resources. This new look will help people more easily find what they need and can also more easily showcase important issues and features.

Privacy continues to be a hot topic and we are regularly asked to speak about it. In this quarter staff presentations included the Government Professionals' Forum, InsideOUT, the Annual Future of New Zealand Government Summit, Alcohol Licensing Inspectors Conference, Local Government NZ and the Woman in Data Science NZ conference.

The Commissioner or our staff have spoken publicly to GP24: the conference of general practice, NZ Parking Association, Simpson Grierson clients and at the Facilities Management Association of NZ conference.

Media enquiries in this quarter included significant topics such as the Police compliance notice, Inland Revenue sharing 'hashed' personal information with social media companies, AI and healthcare and the Manurewa Marae concerns.

Compliance and enforcement

Privacy breaches notifications caused by malicious activity increased this quarter. Such notifications include cyber-attacks, ransomware and unauthorised disclosure for malicious purposes. The potentially 'long tail' of privacy breaches was evident, as one driver of the increase in malicious activity were breaches notified by a telecommunications provider whose systems had been hacked a several years ago.

We are seeing increasing complexity in the issues reported to us. For example, these issues can involve multiple organisations, the use of third party service providers and breaches increasingly impacting larger groups of New Zealanders. This is putting pressure on our small compliance function and we are managing this through continuous risk-based prioritisation.

New Zealand Police have completed all but one of the requirements of the compliance notice issued in December 2021 in relation to the unlawful collection and storage of photographs of rangatahi. The remaining requirement is significant, with Police required to find and delete all unlawfully collected material currently stored on their systems. This requirement is proving difficult to achieve in practice given the scale and organisation of Police's information collections. We have granted the Police an extension until June 2025 to complete the critical task of finding and deleting unlawfully collected images.

We have also been working closely with both Statistics NZ and the Public Service Commission on their inquiries into data misuse allegations at Manurewa Marae. We expect to soon receive matters of privacy concern referred to us from the Public Service Commission Inquiry.

Investigations and dispute resolution

We continue to receive privacy complaints and public enquiries at extremely high levels. The number of privacy complaints requiring investigation this quarter (as opposed to a fast resolve approach) was the highest in two years and has increased our backlog to more than 200 complaints. Public enquiry numbers are also at their highest level in two years.

In light of the constrained resources available to our Office, our approach for complaint timeliness has been to focus on streamlining and increasing the efficiency of our processes. However, this recent increase in complaint volumes has led us to allocate some of our diminishing cash reserves to temporarily bolster this function.

The management of organisational risk

We continue to maintain an ongoing assessment of the critical operational risks that face us and our mitigations. We are currently reviewing and updating our organisation wide risks and the associated risk management architecture.

A core risk for us is lack of impact, resulting in a failure to have privacy treated as a core focus by agencies and a loss of trust and confidence in our Office. In order to address this risk we are continuing to undertake proactive compliance and enforcement activities and to advance our work in exploring and developing additional guidance in the areas of biometrics and children and young people.

Long-term financial sustainability, particularly following the fiscal saving review resulting in a funding reduction of 6.5%, also continues to be an area of high risk for us. The Senior Leadership Team continues to proactively work at identifying areas of savings, whilst

remaining mindful of our ability to deliver a large proactive work programme and reactive core services. As previously reported, increased costs in specific areas adds additional challenges.

The health, safety and wellbeing of our people is also a primary area of focus for our Office particularly as we continue to see an increase in unreasonable conduct from some members of the public. We have been addressing this by holding situational safety training and revisiting our policies covering physical security threats. This is being monitored closely within the Office.

Financial report

We are reporting a deficit of \$71,942 for the three months ending 30 September 2024. This is favourable against a budgeted deficit of \$192,721. The variance against budget is due decreased staff costs as a result of vacancies due to staff resignations, decreases in computer maintenance and network costs. These decreases have been offset by increases specialist services for an independent security review and legal services. We are currently forecasting a deficit of \$479,000 for the year to June 2025. 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.

Yours sincerely

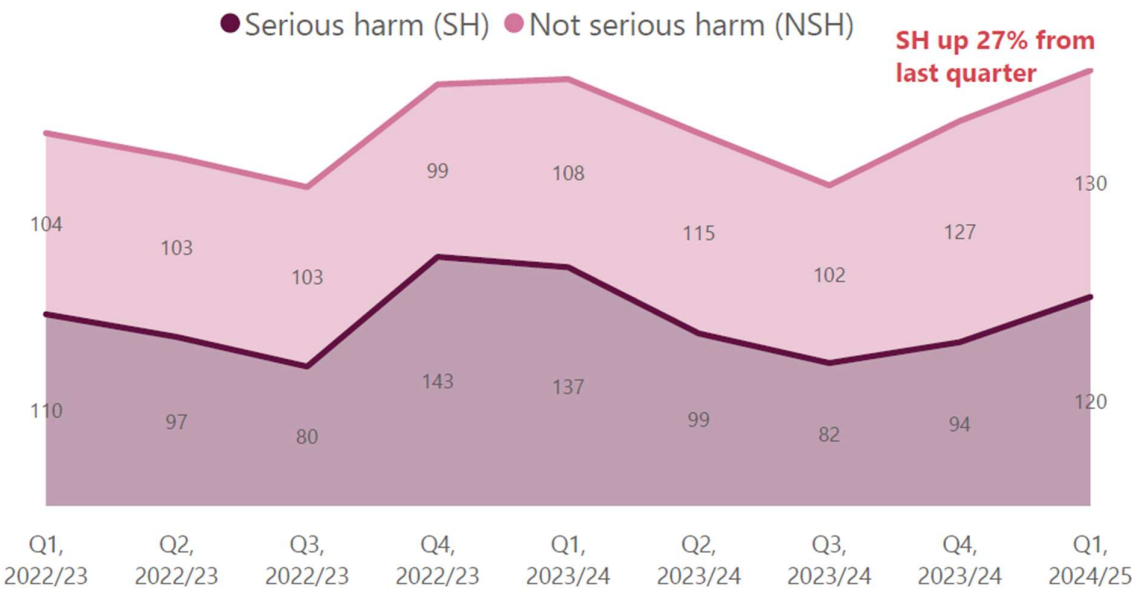


Michael Webster
Privacy Commissioner

Encl:	Appendix A:	Key operational volumes
	Appendix B:	Financials for period ending 30 September 2024
	Appendix C:	Performance against Statement of Performance Expectations - Year to Date
	Appendix D:	Q1 KPI Trend Report – September 2024

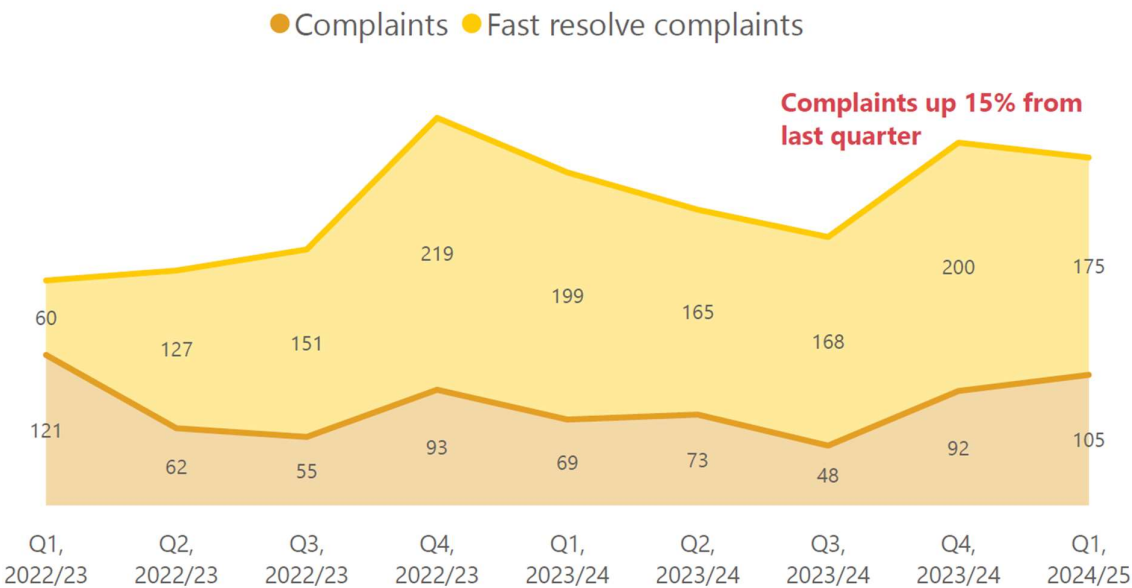
Appendix A: Key operational volumes

Privacy Breach Notifications (from agencies)



Agencies are required to notify OPC of serious/extreme harm data breaches. A single breach can impact a number of individuals for example the Latitude Finance data breach impacted 1 million New Zealanders.

Privacy complaints (from individuals)



Enquiries to our Office

