

30 April 2024

Hon Paul Goldsmith  
Minister of Justice  
Parliament Buildings  
WELLINGTON

Dear Minister

## **QUARTERLY REPORT OF THE PRIVACY COMMISSIONER FOR THE PERIOD 1 JANUARY 2024 TO 31 MARCH 2024**

### **Highlights**

A significant achievement this quarter was the European Commission's January announcement that New Zealand's privacy system continued to provide an adequate level of protection for personal information transferred from Europe. This determination means that New Zealand agencies do not need to put in place additional privacy safeguards when undertaking trade with the European Union. This determination reinforces the importance of the progression of the Privacy Amendment Bill through Parliament.

The past 12 months period has seen the highest volume of privacy breach notifications and privacy complaints on record (see Appendix A for charts). While volumes this quarter were slightly down compared to those in the previous quarter, this pattern also occurred a year ago and was followed by a significant increase in volumes.

The financial sustainability of the Office is an organisational risk we are raising in this update. We are forecasting a deficit of \$180,000 for the year to June 2024 that will be funded by our cash reserves. These reserves can only be applied in the short term before we need to identify and reduce our activities in a way that does not significantly compromise our statutory responsibilities. As noted in our Briefing to the Incoming Minister, without a funding increase (and noting that we have been asked to plan for a 6.5% reduction in funding) this Office will be unable to effectively address the significant regulatory failure occurring across the public and private sectors under the Privacy Act 2020.

Our draft Statement of Performance Expectations for 2024/25 will soon be provided to you for comment. This document sets out three key areas of strategic focus for the 2024/25 year:

1. Continue building our strengthened Compliance and Enforcement function
2. Delivering on our regulatory stewardship responsibilities
3. Ensuring the Privacy Act is fit-for-purpose in the digital age.

## **Developments relating to biometric technologies**

Throughout the quarter the widespread implementation and regulation of biometric technologies has been an ongoing issue that has attracted significant media attention.

### *Foodstuffs trial of facial recognition systems and Privacy Commissioner Inquiry*

On 8 February Foodstuffs North Island began a trial of facial recognition systems in 25 New World and PAK'nSAVE supermarkets for an initial 6 months. The objective of the trial is to help better identify repeat offenders and thereby reduce harmful behaviours in store, thereby helping determine whether Foodstuffs adopts facial recognition systems more widely. This is a novel use of this technology in New Zealand, and our concern is that facial recognition technology is not a proven tool in efforts to reduce harmful behaviour in supermarkets, especially violent harmful behaviour.

We considered our response to this trial and on 4 April formally initiated an Inquiry that will monitor the way stores are running the trial to ensure that it is compliant with the Privacy Act. This Inquiry will also inform the Commissioner's assessment of the effectiveness of the use of facial recognition technology in reducing harmful behaviour. We have also invited comment from the public about how the Foodstuffs trial is impacting them.

On 13 April the media reported on an altercation arising at a New World supermarket participating in the facial recognition trial due to a Māori woman being misidentified as someone who had previously offended at the store. Incidents such as these will be considered as a part of our Inquiry. We note that global evaluations of facial recognition software show that false matches are more likely to happen for people of colour, and particularly for women of colour.

### *Development of a Code of Practice for biometric technologies under the Privacy Act*

Prior to the above, 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. During this quarter we developed an exposure draft of the Code and it was released with a consultation paper for public comment on 10 April.

The exposure draft and consultation paper seek feedback on three main questions:

1. How should organisations have to balance the pros and cons of biometrics before using them?
2. How and what should people be told when their biometrics is being collected?
3. What are some things that biometrics should not be used for?

The consultation period closes on 8 May 2024. We will then review the feedback and make any necessary changes to the draft. There will later be a further period of formal public code consultation before any biometrics privacy code of practice can be issued.

## Activities of our Office

### *Policy*

In addition to the biometric code above, the Policy team analysed and produced a report on the results of our engagement with experts and agencies as a part of our children's privacy work. This engagement revealed three key themes that will help determine the next phase of our work:

1. There is a need for more guidance for parents and children, and for different sectors
2. There is strong concern about children using social media and online risks
3. Regulatory changes are required to improve the protection of children's privacy.

During this reporting period we supported a range of policy initiatives, including:

- the establishment of an Artificial Intelligence work programme
- the development of the Customer and Product Data Bill (the 'consumer data right')
- work led by the Department of Internal Affairs on accelerating the digitising of government services
- Ministry of Justice work on improving New Zealand's electoral law
- the Electricity Authority on improving retail market monitoring.

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

- Gang Legislation Bill
- Firearms Prohibition Orders Legislation Amendment Bill.

### *Capability and guidance*

The key responsibility of this team is a programme of work to overhaul and streamline our guidance to agencies (known as *Poupou Matatapu – Doing Privacy Well*). The objective of this work is to make it easier for agencies to understand how they can do privacy well. Our work is progressing well and during the next reporting period we intend to undertake public consultation on this guidance.

This quarter we launched our updated Privacy Impact Assessment Toolkit, which is a set of guidance and templates to make it easier for agencies to assess the privacy impacts of projects they are undertaking.

Other work undertaken by the Capability and Guidance team during this quarter includes:

- Responding to consultation on access to the Motor Vehicle Register under section 241 of the Land Transport Act
- Responding to a consultation from the New Zealand Customs Service on an additional Information Sharing Agreement under the Customs and Excise Act
- Assisting Immigration New Zealand and the New Zealand Customs Service on a proposed information sharing agreement
- Assisting Te Whatu Ora on large information architecture-related projects they are undertaking
- Collaborating with the Government Chief Privacy Officer to update guidance on Approved Information Sharing Agreements under the Privacy Act.

### *Compliance and enforcement*

The past two months has seen key international markets promote international privacy cooperation, especially for compliance activities. The European Commission convened a Ministerial and data protection agency roundtable on promoting safe data flows for jurisdictions with European Union adequacy status and will be following up with us on specific initiatives. The United Kingdom's Information Commissioner convened a similar group of data protection authorities to discuss working more closely together. Our approach is to be open to proposals with our international counterparts.

In September 2022 we issued a compliance notice to the New Zealand Police while undertaking the *Joint Inquiry into Police conduct when photographing members of the public*. This notice contained 14 requirements of Police that were due for completion by 31 December 2023. The Commissioner has granted a request from Police to extend the deadline of two requirements:

- The identification and deletion of all photographs of young people (and duplicates of photographs) that have been taken in a non-compliant manner
- The identification and deletion of all sets of Biometric Prints (and duplicates of such Biometric Prints) in the Agency's systems that the Agency has collected in a manner that is non-compliant.

Reporting of data breaches by organisations continues its record increase with 479 serious harm breaches reported in the year to 31 March 2024, up 31% from a year earlier. In addition to following up and supporting breached agencies, we are continuing our joint investigation with the Office of the Australian Information Commissioner into the March 2023 Latitude Financial privacy breach. The New Zealand element of the investigation is progressing well and we are currently drafting our preliminary view. As our Office has limited cyber-security expertise, we are leveraging those of the Australian Information Commissioner. We are currently awaiting their cyber-security assessment of Latitude's IT systems of the privacy breach.

### *Investigations and dispute resolution*

This year continues to see high volumes of privacy complaints from individuals, with the 12 months to 31 March 2024 having the highest numbers on complaints on record. There were 1,021 privacy complaints, which is 44% higher than the preceding 12 months (708 complaints).

We settled one matter this quarter that was a representative privacy complaint involving 148 individuals. This complaint related to significant breaches of the right of individuals to access their personal information under Information Privacy Principle 6. The total financial settlement for the file is the highest that has been achieved and exceeds one million dollars.

We are continuing to see high levels of unreasonable conduct from some complainants and we have implemented a number of communications plans for specific individuals in line with our Service Charter, which sets out the principles we follow and the expectations we have for complainants and our investigators.

During this quarter we published on our website *Decision Guide: Investigations and Dispute Resolution*. This guide sets out our decision-making processes when receiving and investigating privacy complaints. Publishing the decision guide will increase the transparency of our processes, which will be especially useful for individuals who are unhappy with the process or the result of their privacy complaint. The decision guide supports other transparency documentation we have on our website.

### *Communication and engagement*

In this quarter the Privacy Commissioner gave keynote speeches to the Project Management conference and National Cybersecurity Summit.

We have been steadily increasing our regular privacy messaging to specific sectors. The Privacy Commissioner wrote his first regular article in the Education Gazette to help teachers better understand privacy implications for children and to provide them with practical tips and advice. Two articles were also written for Management Magazine and one for New Zealand Doctor, concerning AI and primary healthcare.

We have been hosting Ian Axford Fellow Rachel Levinson-Waldman in the Office and introduced her in March with a privacy-themed webinar with the Privacy Commissioner and Deputy Privacy Commissioner.

We provided media comment on a range of issues. These ranged from significant privacy breaches at Te Whatu Ora and Mediaworks, to schools using ChatGPT for marking reports. A variety of stories also related to privacy issues with supermarkets, including CCTV at car parks, loyalty programmes and the Foodstuffs facial recognition trial.

### **The management of organisational risk**

We continue to maintain an ongoing assessment of the critical operational risks that 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. To address this risk, we are undertaking the following activities to set clear expectations of agencies, and to provide them with support on how to meet those expectations:

- exploring the establishment of a Code of Practice for biometrics
- developing a suite of guidance on how to protect the privacy of children, for parents, schools, and other specialists who work with children
- continuing to undertake proactive compliance and enforcement activities, including our recently announced inquiry into Foodstuffs trial of facial recognition technology
- continuing with our work on 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 we have previously advised we are not resourced to effectively address the risk of regulatory failure. The privacy system is increasingly complex and demanding, and while the Office is very active in trying to manage this evolving risk, we cannot do so with current resources.

Relatedly, our financial sustainability following the fiscal savings review is also a high area of risk for the Office. As part of the Office's work on the 2024/25 budget, savings have been identified but increasing costs (such as information technology and rent of premises) are adding further challenges. The Office continues to have sufficient cash reserves and will be utilising this in the short term to fund forecast deficits. The Senior Leadership Team is proactively working to identify additional areas of savings, whilst being mindful to maintain our ability to deliver core services and manage our regulatory failure risk. Our financial sustainability risk may be exacerbated if decisions are not made in the near future on funding of our pending regulatory responsibilities for the Consumer Data Right. Without certainty about funding for this additional responsibility we will need to account for this from our existing funds.

Other areas of high risk include the possible failure to target our activities for maximum impact, cyber risk, and meeting our statutory responsibility to take account of cultural perspectives on privacy. Mitigations have been identified for these areas and are being enhanced where needed.

### **Financial report**

We are reporting a net surplus of \$84,138 for the nine months ending 31 March 2024. This is in excess of the net surplus budgeted of \$13,283 as a result of decreased staff costs due to staff resignations offset by increases operating costs particularly in computer maintenance and network costs. We are currently forecasting a deficit of \$180,000 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.

Yours sincerely

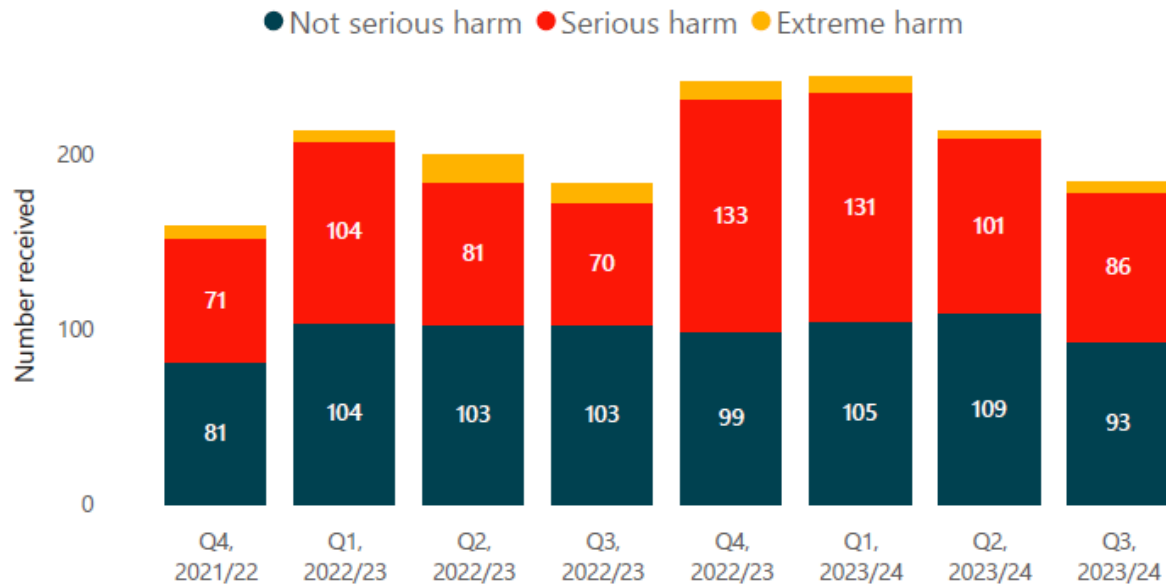


Michael Webster  
**Privacy Commissioner**

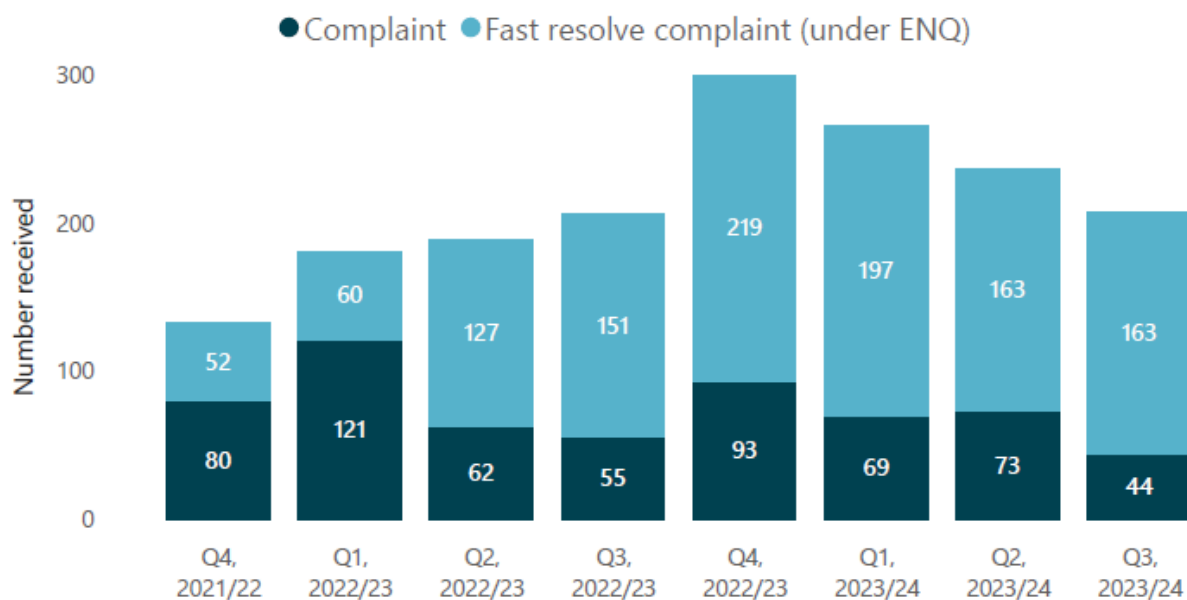
Encl:	Appendix A:	Key operational volumes
	Appendix B:	Financials for period ending 31 March 2024
	Appendix C:	Performance against Statement of Performance Expectations - Year to Date
	Appendix D:	Q1 KPI Trend Report – March 2024

## Appendix A: Key operational volumes

### Privacy breach notifications (from agencies)



### Privacy complaints received (from individuals)



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.

## Public enquiries incl. Call Centre (from individuals)

