



Privacy Commissioner
Te Mana Mātāpono Matatapu

STATEMENT OF INTENT

1 JULY 2020 TO 30 JUNE 2024

Contents

Foreword	2
About this document	3
Our role and the context we operate in	4
The role of the Privacy Commissioner	4
Our mission.....	4
Our core functions and responsibilities.....	4
Our values	5
Justice sector and Government priorities	5
Our external environment and how we interact with others.....	7
How New Zealanders feel about their privacy	7
The wider privacy system.....	7
How we work with others in the privacy system.....	8
Our challenge	15
Data protection challenges are constantly evolving.....	15
Becoming a more modern and effective regulator	15
Our response to the challenge in a nutshell	15
Our strategy	17
Our strategy on a page.....	17
Our objectives: What we want to achieve	18
Privacy protection is effective and easy to achieve	18
The costs of privacy compliance are minimised	18
The OPC is trusted as a fair and responsive regulator	18
The OPC influences privacy practices and behaviours.....	18
Our priority actions: What we will do to achieve our objectives	19
Making evidence-based decisions	19
Aligning our business plans with our overall strategy	20
Monitoring compliance and enforcement.....	21
Monitoring the effectiveness of our interventions.....	22
Strengthening our reputation as a trusted, effective regulator	23
Advocating for privacy.....	24
Our enablers: What we need to be able to work effectively.....	25
Operations organised around primary activities	25
Functions work together as inter-related system	26
Effective systems, technology and processes	29
Highly skilled and engaged staff.....	29
Effective strategic engagement with stakeholders.....	29
Meaningful performance measures	30
Equal Employment Opportunities and Good Employer Statement	30

Foreword

Globally, governments are recognising the challenges of regulating new data-driven industries and a data economy where the transactions and interactions of each of us support multi-billion-dollar businesses.

Those businesses extend beyond the borders of nation states; they move fast and break things, innovate at the speed of fibre optic broadband, deliver fantastic services that improve the lives of billions, and leave regulators in the dust; unable to keep up, unable to match their resources, unable to assert effectively that their 'one size fits all product' does not in fact, fit all.

There is no easy solution. There are over 100 data protection and privacy commissioners working nationally and other regulators working in-country, providing independent regulation in a patchwork quilt of domestic laws. Against this backdrop of constant change, privacy and data protection regulators are facing unprecedented demand – whether through new privacy invasive technologies or rapidly emerging issues requiring new information collections such as Covid-19 – for advice, guidance, well-targeted policy interventions and commentary.

Our mission is to meet these demands to be an effective, modern privacy regulator – both in New Zealand and internationally. We will promote flexibility, transparency and intelligent application of our resources to maximise our responsiveness and influence and increase citizen awareness of privacy challenges. We will reconceive our operational approach to better respond to these challenges. We will be bringing together insights and intelligence from our operations and experience to inform our strategic approach.

In practice, we work alongside government and business to ensure new developments achieve their objectives, while also treating the information of citizens and customers with respect. We seek to reach pragmatic and workable solutions that support the privacy interests of each of us.

The Privacy Act 2020 gives the Privacy Commissioner a greater range of enforcement powers, including the ability to issue compliance orders, and to issue access determinations. Businesses and organisations now have clearer obligations to report to affected people when things go wrong with customer or client data.

We must always keep the wider context in view, and we will coordinate with our international colleagues to achieve the greatest impact for New Zealanders. Locally, we will make greater efforts to partner with Māori as tangata whenua, and act to protect personal information as taonga for all New Zealanders.



John Edwards
Privacy Commissioner

30 June 2020

About this document

This four-year Statement of Intent (SOI) is prepared in accordance with the Crown Entities Act 2004 and is supported by the Statement of Performance Expectations (SPE) which is updated on an annual basis. Both of these documents should be read concurrently in order to get a full understanding of both the long-term strategic objectives of the Office and the shorter-term targets set on an annual basis.

This SOI provides an overview of the current environment in which the Office operates and sets out the strategic direction over the period 1 July 2020 to 30 June 2024. It also provides an overview of how the Office will use its resources to meet its strategic objectives and prioritise work over the four-year timeframe and how it intends to measure its performance against these objectives.

Our role and the context we operate in

The role of the Privacy Commissioner

Our mission

Our mission is to be an effective, modern privacy regulator – both in New Zealand and internationally. That means:

- We understand the privacy system and our external environment, and we act independently as a leader and regulator.
- We promote transparency around organisational privacy practices and compliance, and increase citizen awareness of privacy challenges by making privacy easy.
- We are adept at working with our stakeholders to develop and promote a culture in which personal information is protected and respected.
- We proactively address privacy issues by talking about it in the media and public forums and we lead the thinking around the future of privacy in New Zealand and internationally.
- We partner with Māori and act to protect personal information as taonga for all New Zealanders.

Our core functions and responsibilities

The OPC has a wide range of functions. Key areas of work include:

- Making public statements on matters affecting individual privacy.
- Investigating complaints about breaches of privacy.
- Building and promoting an understanding of the privacy principles.
- Monitoring and examining the impact that technology has on privacy.
- Developing codes of practice for specific industries or sectors.
- Examining draft legislation for its possible impact on individual privacy.
- Monitoring data matching programmes between government departments.
- Inquiring into any matter where it appears that individual privacy may be affected.
- Receiving reports of notifiable privacy breaches.
- Monitoring and enforcing compliance with the Privacy Act.
- Reporting to government on matters affecting privacy, both domestic and international.

Our values

Respect – *Whakaaro nui*

For all the people we deal with, and for viewpoints that differ from our own.

Ki ngā tāngata katoa e mahi ana me mātau, me ngā whakaaro rerekē ki ō mātau ake

Integrity – *Ngākau tapatahi*

We are honest, fair and transparent in our work.

He pono me te matatika mātau me te ngākau tuwhera i roto i ā mātau mahi

Independence – *Motuhaketanga*

We operate impartially and without political or personal bias.

Ka mahi mātau i runga i te wairua tōkeke me te kore e riro i te whakaaro tōrangapū, whaiaro rānei

Innovation – *Auahatanga*

We value innovation, creativity and a culture of continuous improvement.

He hira ki a mātau te auahatanga, wairua auaha, me te wairua rapu kia pai haere tonu

Excellence – *Hiranga*

We strive for best professional practice and leadership in our field.

Ko ngā tikanga tino ngaio tā mātau e whai ana me te noho mātāmua i roto i tō mātau rāngai

Justice sector and Government priorities

While recognising the Privacy Commissioner's independence from government the Statement of Intent aligns with the Minister's Justice Sector priorities as well as Government's priorities

The Government's priorities are to put the wellbeing of people and the environment at the centre of what it does, and to introduce policies that will allow the economy to work smarter and make better use of our resources, and to ensure that the benefits of growth are spread more evenly across society.

The Ministry's vision is for safer communities with increased trust in the justice system, for the wellbeing of everyone as a core priority for the justice system, and for the integrity of our constitutional arrangements to be maintained.

The Privacy Commissioner will contribute to these priorities by strengthening privacy protection for individuals and helping ensure that agencies comply with the law and good personal information practices.

The Statement of Intent supports expectations.

- To efficiently enforce agencies, compliance with the new mandatory breach notification requirements to ensure better accountability by agencies and greater protection of personal privacy,
- To utilise the new ability to issue compliance notices to address systemic issues before they cause any further harm,
- To assess, on request, the privacy safeguards of other countries and cross-border binding schemes against criteria and express an opinion as to whether those safeguards are comparable to New Zealand's,
- To monitor and report on authorised data matching programmes, and information sharing across government, including the provision of advice to agencies carrying out information sharing and matching, and
- To continue to be active in international forums in the Asia-Pacific region and European Union countries to ensure that New Zealand is recognised as having privacy protections suitable for acceptance by the international community.

Our external environment and how we interact with others

How New Zealanders feel about their privacy¹

More than half (56 percent) of all New Zealanders are more concerned with their individual privacy now than they were in the last few years, as indicated by a public attitude survey carried out for the Privacy Commissioner.

New Zealanders were most concerned about businesses sharing personal information with other businesses (75 percent with just 8 percent unconcerned) followed by Security of banking and credit cards and online personal information security (both at 72percent).

The proportion of respondents who have heard of the Privacy Commissioner was 73 percent while awareness of the Privacy Act was 81 percent.

The wider privacy system

The privacy system encompasses every part of the economy that involves personal information.

Our system outcomes

We work with agencies, businesses, government and regulators to achieve key privacy outcomes:

- Individuals can be confident that their privacy is protected, and they can make informed choices.
- Businesses have trust and confidence in the system, and it supports their growth and innovation.
- New Zealand government promotes and supports individual privacy rights in their interactions with citizens. Agencies are empowered to use data in a privacy protective way for the benefit of the public.
- Overseas governments have trust and confidence in our privacy system.

We contribute to broader outcomes such as:

- Upholding human rights.
- Protecting individuals.
- Supporting trade.
- Advocating for better privacy practices internationally.

¹ “*Privacy concerns and sharing data*” Omnibus research commissioned by the Privacy Commissioner. UMR April 2020

How we work with others in the privacy system

We work for and with others to achieve the best privacy outcomes for New Zealanders.

Citizens

We increase citizens' awareness of privacy challenges by showcasing good practice and calling out the bad. We reach out to young New Zealanders to make sure they understand how to protect their privacy and understand their rights. We use industry bodies and associations as multipliers, making sure relevant messages reach as many people as possible.

When citizens come to us with direct enquiries, complaints, or notifications of potential privacy breaches, we find a swift and appropriate response that protects the privacy interests of individuals, addresses the underlying reasons for the particular conduct or incident, and mitigates risks to other New Zealanders. This can take the shape of:

- **Communicating and educating:** Individuals receive material to inform, guide and educate their privacy practices and behaviours.
- **Resolving disputes:** We do our best to resolve or settle disputes between the parties involved in a complaint.
- **Enforcing compliance:** If an individual complaint indicates systemic problems, we investigate those and work with all the parties involved to enforce and monitor compliance.

Māori and Privacy – applying a Te Ao Māori lens

We recognise that to be an effective privacy regulator in Aotearoa New Zealand we need to be able to walk in a Te Ao Māori world and consider privacy through a Te Ao Māori lens. We acknowledge that we are at the beginning of our journey in this area. Over the course of the next four years we will:

- Continue to build and support the capability and confidence of staff to engage effectively with Māori and in Te Ao Māori through training in te reo Māori, tīkanga and kawa
- Develop effective mechanisms to help us identify and mitigate any cultural bias in our decision-making
- Seek to develop effective, te Tiriti-based relationships with Māori and Iwi organisations including with the National Iwi Chairs Forum's Data Iwi Leadership Group, Te Mana Raraunga (the Māori Data Sovereignty Network)
- Work in partnership with Māori to develop a strategy and framework for applying a Te Ao Māori lens to privacy issues.

CUSTOMER JOURNEY CITIZEN



John Smith
NZ citizen:

“I hope the government takes care of my data”

Expectations

I know who holds my data and why. My privacy is protected.

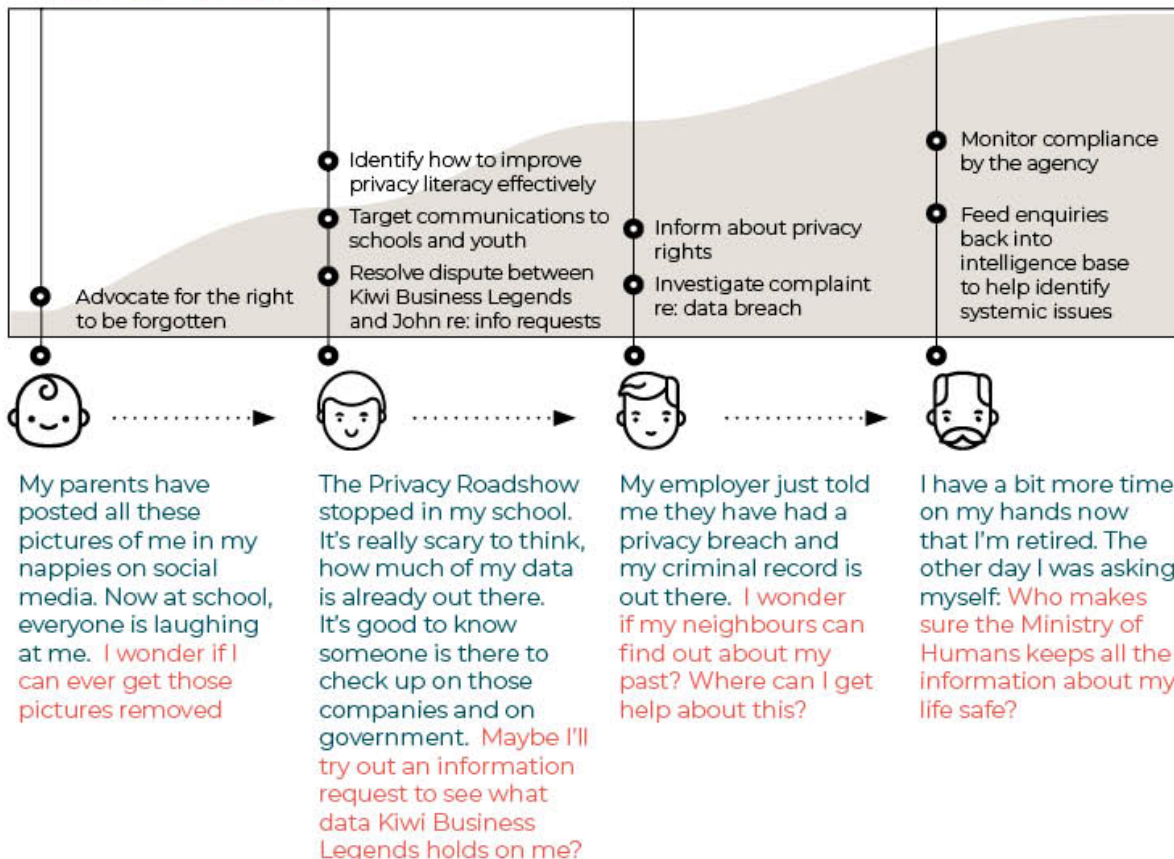
Experiences

The different platforms and apps that use and share data are not transparent.

Views and perspectives

To live a normal life, I have to share my data with heaps of government agencies and companies. I don't understand all the terms and conditions I'm signing.

What the OPC does



Government agencies

We make sure that we inform public sector agencies about their obligations, give them guidance, and promote best-practice approaches that help them improve their privacy outcomes. We partner with others like the Government Chief Digital Officer to assess and improve privacy maturity across government.

The information and education material we provide, like brochures and eLearning modules, help organisations help themselves. We also work alongside agencies to workshop good solutions and develop training programmes.

We also partner with specific agencies, such as the Ministry of Health, to address particularly sensitive challenges to privacy in their specific area of work.

When compliance issues arise, we work closely with the agency:

- Informing and supporting it through the appropriate procedures and steps.
- Recommending how the agency can improve compliance.
- Monitoring its compliance and implementation of our recommendations.

CUSTOMER JOURNEY PUBLIC SECTOR



Ministry of Humans
Public agency:

“We’ll take all the help we can get to ensure our policies and practices are sound”

Expectations

OPC and the Government Chief Privacy Officer will work together and help me improve my organisation’s privacy maturity.

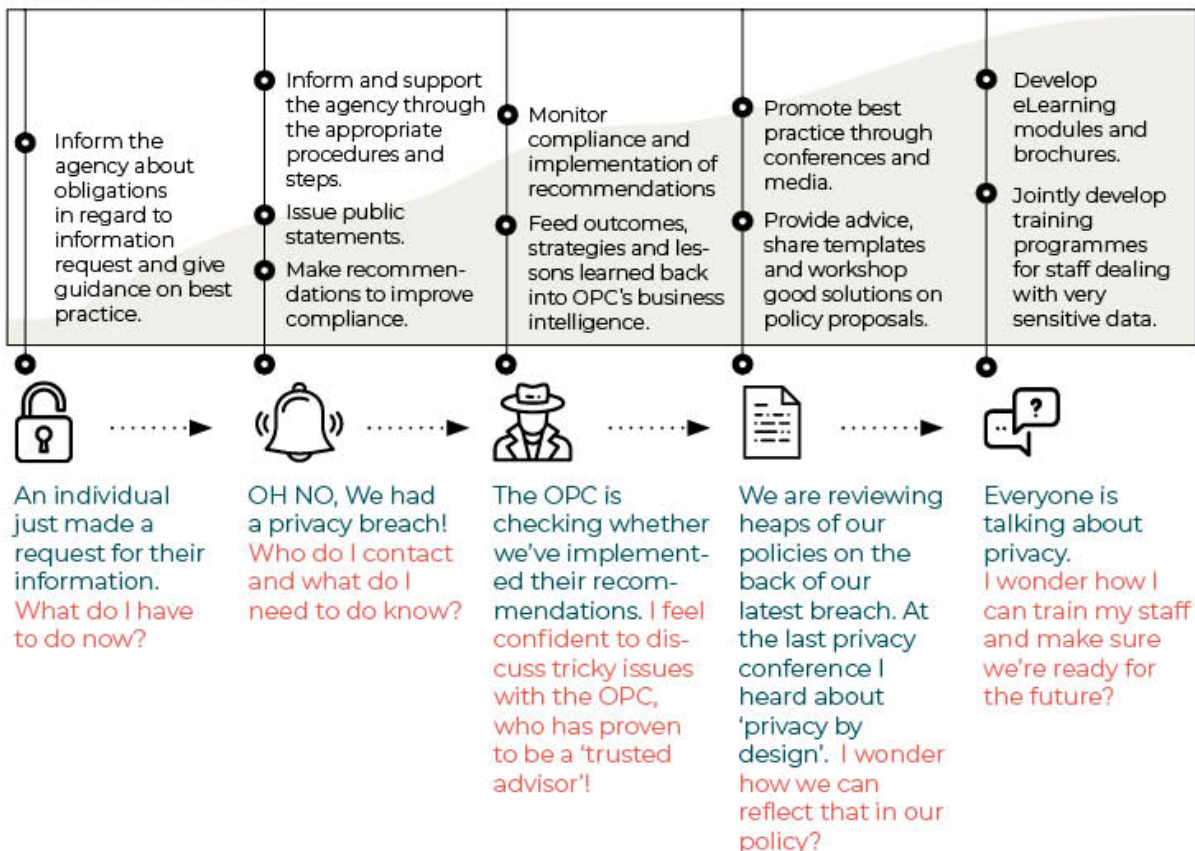
Experiences

It’s really hard to get privacy experts to join our team. We’ll need to invest in informing and educating our team.

Views and perspectives

We had a pretty bad privacy breach last year. We were in the media for weeks and got a lot of heat from our Minister. I don’t ever want to experience that again.

What the OPC does



Businesses

We develop training and information material that reflects the working environment of businesses – from small companies to large corporations.

We support Privacy Officers and teams of large organisations in assessing and improving their privacy maturity and identifying their recurring and systemic issues. We advise organisations on best practice and we partner with industry bodies and large corporations to advocate for good privacy outcomes.

We work with the Ministry of Business, Innovation and Employment to ensure small and medium-sized organisations, including in the regions, understand their responsibilities. The 'starter kit' is easy to find on our website, and entrepreneurs find it easy to find the right people to contact.

CUSTOMER JOURNEY BUSINESS



Kiwi Business Legends Inc.,
Corporation:

“We’ve grown a lot in the past few years. Our policies and practices need to reflect our bigger role in the NZ economy”

Expectations

The OPC will assess our privacy policies and practices and advise us on how we can improve

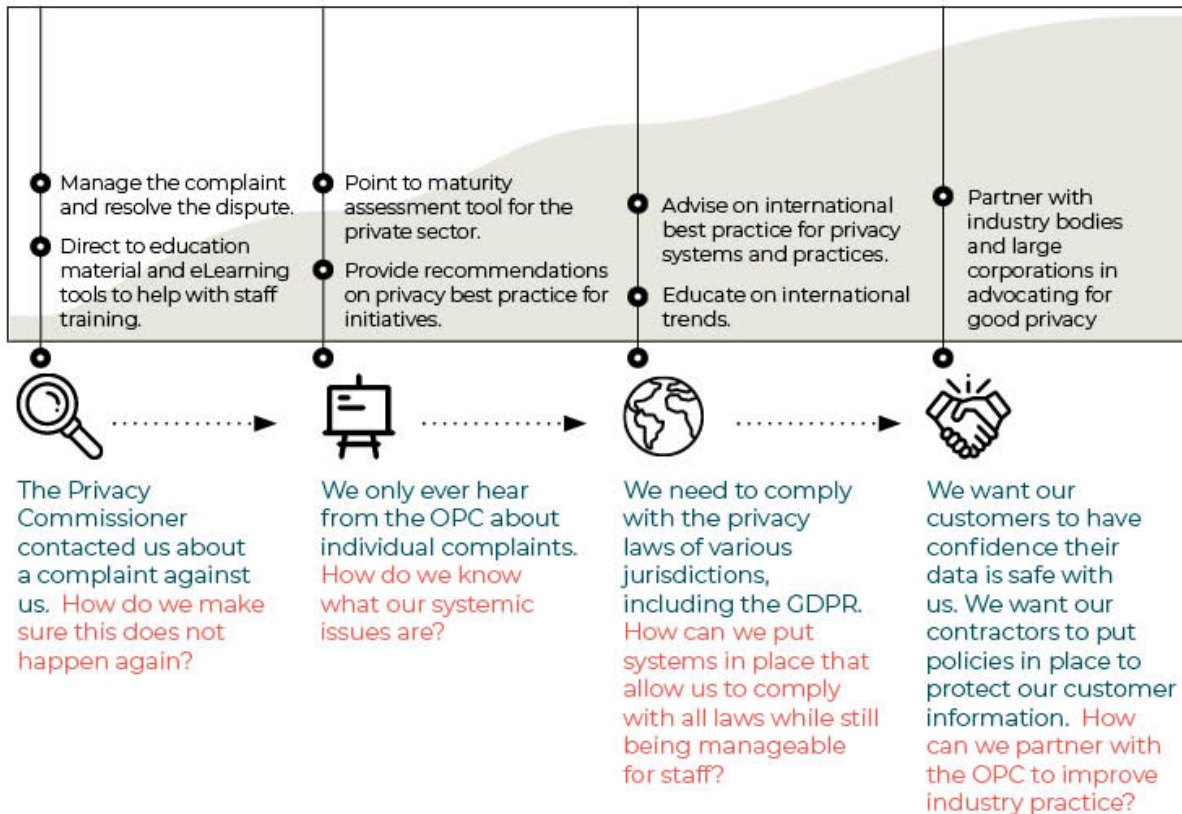
Experiences

We only hear about individual complaints. It’s hard to understand the ‘big ticket’ issues we need to address across our organisation.

Views and perspectives

We are a big organisation now and have a responsibility to both our employees and our customers to handle their information with care. We have a reputation to protect!

What the OPC does



Sectors and associations

We liaise with industry bodies and associations and build on collective insights to find the best platform to get relevant messages to the right audience.

The national and international privacy system

We build and improve multi-stakeholder networks and increase our influence to improve personal information practise. We have a reputation as an agile, skilled and effective regulator – both nationally and internationally. We are seen as a leading privacy regulator globally.

That includes:

- Being strategic about participating in conferences and international speaking engagements.
- Liaising with thought-leaders in the privacy space in New Zealand and internationally.
- Building networks and cooperating with other jurisdictions to continually assess technological developments and their impact on individual privacy.
- Partnering with the Human Rights Commissioner.

Our challenge

Data protection challenges are constantly evolving

Our Office is operating in a rapidly evolving environment. Given the underlying importance of privacy to individuals and faced with the challenges that a rapidly changing environment present, New Zealanders have the right to expect a privacy regulator that:

- Protects their rights and interests both at an individual level and societal level.
- Holds agencies to account or provides individuals with the tools to take their own action where appropriate.
- Adapts to challenges that may not have been in contemplation when its legislation was passed.
- Understands, comments and provides advice on technological changes, promoting global best privacy practice.
- Engages with Māori on their privacy, including special interest areas like data sovereignty.

Becoming a more modern and effective regulator

To meet the expectations of us, we need to update how we work and operate as a modern and effective regulator i.e. with flexibility, transparency and intelligent application of our resources to maximise our responsiveness and influence.

The Privacy Act 2020 has given the Privacy Commissioner a greater range of enforcement powers, including the ability to issue compliance orders, and to issue access determinations. The Act was modernised, and businesses and organisations now have clearer obligations to report to affected people when things go wrong with customer or client data.

We decided to combine our new responsibilities with a new approach to how we operate – rather than just bolting our new responsibilities onto our existing operating model. If we failed to change, we would risk losing our relevance and the trust of New Zealanders which, at its worst, would lead to us failing as a regulator. It marks a first step in an exciting and important new chapter for the OPC.

Our response to the challenge in a nutshell

We are moving from focusing mainly on individual harm, to identifying systemic issues, being aware of potential harm and intervening early. As an effective and modern regulator, we aim to focus on the broader public benefit of privacy protection.

This means:

- Using all inputs to the Office to inform our strategy.
- Increasing our awareness of our operating environment and gathering data so that our decisions are better informed and so we better understand emerging challenges.
- Applying more resource to compliance and enforcement work.

- Developing clear frameworks for assessing which work has the highest public benefit.
- Making choices that make privacy accessible and privacy issues understandable and relevant to all New Zealanders.

This strategy document explains how we will work over the next four years to make that transition successfully:

- **Our objectives** describe how we create public and economic benefit and work towards increasing the wellbeing of New Zealanders.
- **Our priorities** draw out what we will need to focus on in the next four years to achieve our objectives. We will illustrate why we chose these priority areas, what we will do and what success looks like to us.
- **Our enablers** look at how the organisation needs to be set up to achieve our objectives and priority areas. They outline how we will strengthen or develop our organisational capability in key areas.

- The biggest change the Office has initiated is moving towards organising its operations around the primary activities it needs to perform: Strategy and Insights, Communication and Education, Compliance and Enforcement, Advice and Advocacy, and Investigations and Dispute Resolution.

The activities support the Office in operating as an inter-related system. The work of individuals and individual teams fit into the bigger picture and contribute to achieving shared objectives. Thinking more systemically helps the Office allocate and prioritise resources more effectively. It brings various perspectives and insights to decision-making and facilitates coordinated action.

- To understand and maximise our impact we need the right information, technology and systems to enable us to work in a smart, strategic, integrated way. This will be the foundation for producing robust analytics and insights and strengthening our evidence-based decision making.
- People working at OPC are passionate about privacy and dedicated to promoting it. We need to continue building and valuing a strong organisational culture that ensures our people feel engaged and valued.
- We are part of a wider privacy system and need to work with and through others to ensure we are as effective as we can be. Connecting with national and international regulators enables us to pool resources, share wisdom and practice, and to learn from others.
- In order to improve individuals' privacy outcomes, we need an in-depth understanding of the effectiveness of our interventions. We will collect insights and monitor our work against meaningful performance measures.
- The mandate of the Privacy Commissioner sets the framework for our work, as reflected in **our mission, core functions and our values**.
- Our **external environment and how we interact with others** describe how we work within our environment to achieve good privacy outcomes.

Our strategy

Our strategy on a page

Our mission

Who we are:

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

Our objectives

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



Our primary activities – What we will do:



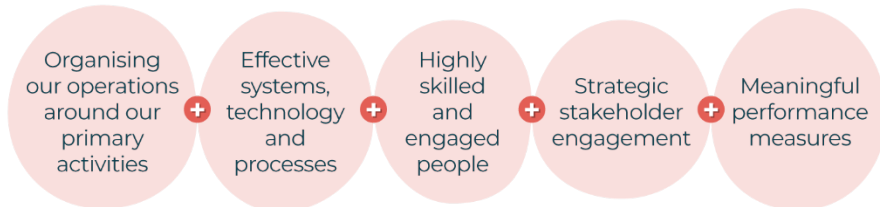
Our priorities

What we'll focus on:



Our enablers

What we need to get there:



Our values

While upholding our values:



Our objectives: What we want to achieve



Privacy protection is effective and easy to achieve

When there is effective privacy protection and it is easy to achieve, individuals engage in society knowing their privacy interests are being protected and promoted. At the same time, organisations are empowered to use personal information in ways that respect privacy and that are commercially or socially beneficial.

Making privacy easy makes it accessible and empowers people and organisations to lift their level of compliance and exercise their rights.



The costs of privacy compliance are minimised

The decisions we make as we oversee compliance with the Privacy Act can have commercial ramifications for individual agencies or for parts of the economy. The Act obliges us to recognise the right of government and business to achieve their objectives in an efficient way.

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



The OPC is trusted as a fair and responsive regulator

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

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



The OPC influences privacy practices and behaviours

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

We exert that influence in a range of ways: the way we communicate, the cases we choose to take, the outcomes of those cases, and the data we produce to support our positions.

Our ability to influence is key to making sure privacy is a central concern for government when it creates and implements policy and law.

Our priority actions: What we will do to achieve our objectives

This section sets out what we want to focus on in the next four years in order to achieve our objectives. It also sets out our immediate actions for the next 12 months.

Making evidence-based decisions

We will advance our evidence-based decision making so that we get the best privacy outcomes for New Zealanders

Why this matters

We have a wide remit and finite resources. In order to apply those resources most effectively and efficiently, we need to decide and act on the basis of sound evidence.

What we will do

In the next four years, we will focus on harvesting data, collating information and developing our capability to identify and prioritise the areas where our interventions have the most public benefit.

What success looks like

- We have the tools and expertise to access and analyse information from a range of sources, to inform our strategic decision-making.
- We have robust decision-making frameworks that support staff in prioritising the most important work.
- Rapid prioritisation and allocation of work allows timely responses and sets clear expectations about what work the Office will and won't be resourcing.
- The Office is aware of and can respond to emerging behaviour and technological trends in order to set behavioural expectations and produce compliance, or to inform future enforcement work.

Aligning our business plans with our overall strategy

We will strengthen strategic business planning across our Office, to allow us to take cohesive, targeted action

Why this matters

To achieve our mission as New Zealand's privacy regulator, we must be clear about our focus areas and revisit regularly the strategic business plans of our functions and teams.

As well as providing internal clarity and informing our business reporting practices, well-formed business plans also help us explain to our audiences how we have set our agenda.

Our strategic business plans help us measure our performance and identify weaknesses in our strategic and tactical responses.

What we will do

In the next four years, we will put systems and practices in place that ensure that the plans of the different parts of the Office are aligned and form a cohesive whole. This will allow us to be more systematic in taking joint actions to address priorities we have identified, such as in specific industry sectors or about specific types of data breaches.

Our strategic business plans will be informed by an evidence base and are discussed across the leadership team.

Strategic business planning across functions is an ongoing iterative process. The relevant objectives and key results need to be revisited regularly.

What success looks like

- Staff are clear about their roles and about the value they bring to the Office and the privacy outcomes they contribute to.
- We can measure our performance against a strategic plan, and shortcomings are addressed if objectives have not been met.
- We think systemically about our functions and are therefore able to identify roadblocks or resourcing needs.
- We are able to communicate a clear rationale for how we prioritise the work that comes into the Office.

Monitoring compliance and enforcement

We will strengthen our compliance monitoring and enforcement capability, so that we are better able to hold organisations accountable for their privacy practices

Why this matters

To succeed as an effective, modern regulator, we need to be able to make good choices about how we respond when we have identified an issue as a priority area.

Compliance work is often preventative, addressing conduct before it becomes a problem and so reducing the impact on individuals. This requires the intelligent use of our full suite of tools for influencing behaviour and enforcing compliance.

In some cases, for example where conduct is particularly serious or we want to set firm expectations in an area, we may choose to use our statutory enforcement powers. In other cases, we may decide that education or public comment is all that is needed to achieve the best outcome for New Zealand in the most effective way.

What we will do

In the next four years we will focus on putting systems and practices in place to allow us to make intelligent tactical decisions.

What success looks like

- Our compliance capability is supported and informed by other functions within the Office, in particular the Strategy & Insights capability.
- We can measure the impact of our compliance work and can link this to public benefits.
- Our compliance responses are found to be proportionate and effective.
- Our enforcement action achieves our strategic aims for enforcement.

Monitoring the effectiveness of our interventions

We will monitor our performance and the effectiveness of our interventions and take corrective action when needed

Why this matters

A culture that supports ongoing feedback and performance monitoring is critical to ensuring we are making the best decisions about how to apply our resources. We may not always get it right, and it is important to be able to recognise where we don't get it right and modify our approach to improve our effectiveness.

What we will do

In the next four years, we will further improve our ability to assess how our inquiries and other interventions were received and what their impact has been.

What success looks like

- Ongoing feedback and reviews are baked into our compliance and enforcement processes.
- We think about outcomes and measure effectiveness at all stages of our work.
- Our systems and data analytics processes support ongoing feedback and monitoring.
- Our culture supports reflecting on outcomes and on recommendations from feedback or monitoring.

Strengthening our reputation as a trusted, effective regulator

We will continue to foster a deserved reputation as a regulator that provides expert guidance, communicates effectively, and responds to issues and trends promptly and effectively

Why this matters

Demonstrating that we are a modern, effective regulator that government and citizens can rely on is critical for maintaining and building New Zealanders' trust and confidence in us. In turn this increases our ability to influence others in the wider privacy system and use that influence to achieve good privacy outcomes.

Our reputation for fairness helps maintain trust that we are acting in the public interest and means our audience listens when we speak.

What we will do

As a modern regulator we will always carefully consider the consequences of our actions, seek input where appropriate, and keep proportionality and commercial common-sense front of mind.

A key part of being an effective regulator is being an effective communicator. We have a wide range of audiences, with different needs and levels of understanding. By simplifying what can sometimes be complex legal concepts we speak to our audiences using appropriate language and tone.

Our immediate next steps in this area will focus on the transition to the new Act. We will ensure that we are – and are seen to be – well-prepared for the new statutory regime and able to provide clear and expert guidance on rights and obligations under it.

What success looks like

- Our responses are perceived as fair, and we engage with our audiences in a transparent way.
- Our expert advice is valued across government and business and we are consulted on relevant questions early.
- Our international counterparts seek our advice and opinions.

Advocating for privacy

We will advocate for best-practice approaches to privacy and to legislative reform

Why this matters

In order to promote privacy, we need to be advocates for it. Effective advocacy sends signals about where the Office sees the need for behavioural change. It provides information and raises awareness of privacy issues with people and agencies. In some instances, it is an important precursor to compliance or enforcement work, sign-posting issues to give agencies time to address them. Advocacy also indicates where the Office sees the need for system-level change (such as law reform).

What we will do

To be an effective advocate for privacy in New Zealand and to make sure our message is not diluted or confused, we will apply our resources in the areas where we can be most effective.

What success looks like

- We have a shared understanding of our position on relevant issues and can use this understanding to advocate at all levels of the organisation.
- We speak with integrity, respect and independence.
- We target the right audience with the right message at the right time.
- We are innovative and collaborative in our advocacy and our communications.
- We think broadly about our advocacy role and recognise all opportunities to promote privacy.

Our enablers: What we need to be able to work effectively

To achieve our priorities, we will strengthen or develop our organisational capability in five critical domains.

Operations organised around primary activities

The Office’s functions, listed below, are divided into primary activities, that is, all those tasks the Office needs to perform to deliver on its mandate, and critical cross-cutting activities.

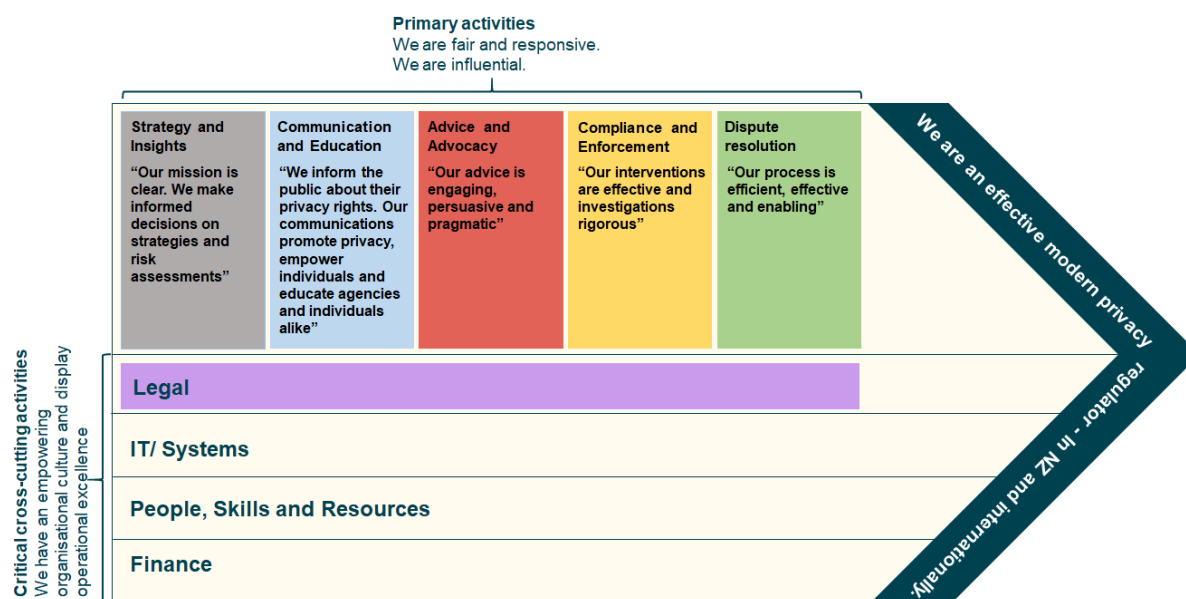


Figure 1: Functions

Primary activities

Strategy and Insights: Understanding trends and technological developments that will be relevant in the future. Using evidence based on all inputs, including complaints, media, breach reporting, enquiries, international regulators or website analytics, to prioritise work and make decisions. Monitor success of strategies and initiatives. Advising the Commissioner on the best way to achieve the Office’s mission as well as associated risks.

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

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

Advice and Advocacy: Research and analysis supports advice on privacy issues that is context aware, evidence based and clear and informed. Advice reflects diverse perspectives and recognises risks and competing interests. Effective interventions include the

development of privacy codes and advice to government on changes to other legislation. Advocate for privacy positive outcomes, including privacy by design.

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

Corporate Service: Provide human resource, finance and office management function to enhance service delivery and the welfare of all staff. Manage, monitor and assess performance. Manage relationships with external providers and provide IT systems and functionalities to support effective case management.

Legal: Provide legal advice across all primary activities. Lead litigation under the new Act. Legal advice and drafting expertise for code development.

Functions work together as inter-related system

The workflow key functions diagram illustrates how the functions support the Office in operating to deliver on the primary activities as an inter-related system. It shows how the work of individuals and teams fit into the bigger picture and contribute to achieving our shared objectives. Thinking more systemically will help the Office allocate and prioritise resources more effectively. It helps bring various perspectives and insights to decision-making and facilitates coordinated action.

We aim to achieve seven outcomes:

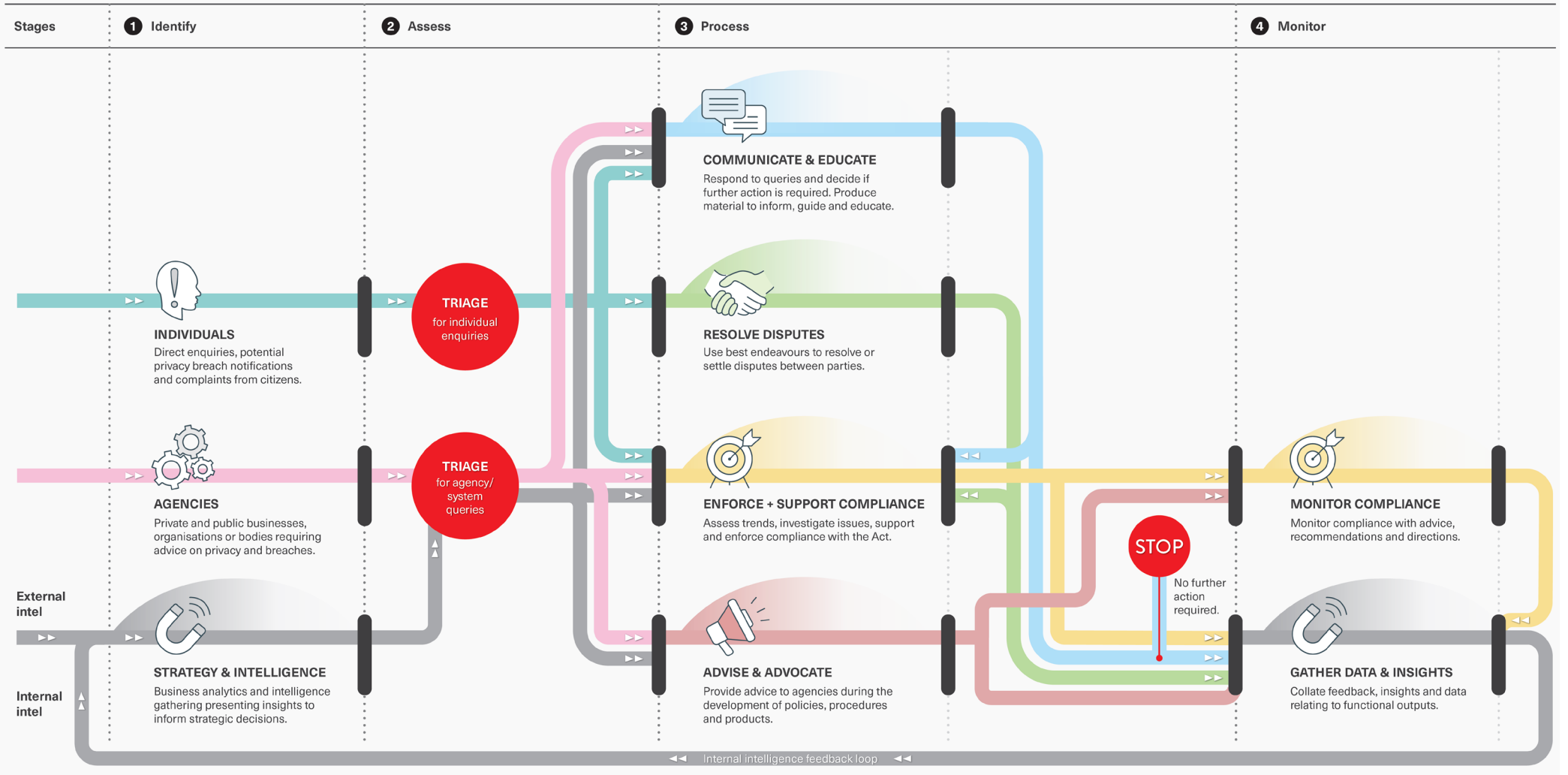
- A Strategy & Insights function enables the organisation to keep a finger on the pulse of privacy issues and engage in evidence-based decision making about resource allocation.
- The Strategy & Insights team and the Compliance & Enforcement team work closely with the Investigations and Disputes Resolution team to identify and act on systemic or sector-specific issues that generate multiple individual complaints.
- The Communication & Education function gains resource to focus more on strategic engagement and education. More effort is put into cultural and Māori engagement.
- The Advocacy & Advice function focuses on finding the right policy responses to sector-specific challenges and technological developments. The team liaises with international regulators, identifies best-practice approaches or benchmarks, and leads efforts to advocate for privacy positive outcomes.
- A Compliance & Enforcement function marks a shift from an individual-based complaints approach to a system-wide approach that considers privacy outcomes at a societal level. It improves the OPC's ability to assess the privacy maturity of organisations, give advice, and take the most effective actions.
- The Investigations and Dispute Resolution function has a greater focus on decision-making on how to best proceed with incoming complaints. In some cases, the OPC might decide not to fully investigate complaints that could amount to an interference with privacy, but to provide the complainant with the opportunity to access the

Human Rights Review Tribunal (HRRT). The outcomes of the initial assessments will inform the identification of systemic issues.

- The OPC focuses on assessing and prioritising work in a cross-functional way.

WORKFLOW KEY FUNCTIONS

- Strategy and intelligence
- Communication and education
- Dispute resolution
- Compliance and enforcement
- Advice and advocacy



Effective systems, technology and processes

To understand and maximise our impact we need the right information, technology and systems to enable us to work in a smart, strategic, integrated way. This will be the foundation for producing robust analytics and insights, strengthening our evidence-based decision making.

We aim to achieve three outcomes:

- Effective content management (CMS) and customer relationship management (CRM) systems ensure our people have the tools and technology to do their jobs well. Leveraging these technologies will enable us to improve how individuals, businesses and agencies access, use and experience our services.
- Data collection and analysis practices support us in taking a more coordinated and deliberate approach to the use of data, intelligence and evidence, including research and evaluation. This is critical for targeting our activity and understanding the effectiveness of our interventions. We will strengthen our data and analytics to improve our knowledge of how the privacy system is performing.
- We will use technology to make our internal processes more efficient, including investing in a Human Resource Management system (HRIS).

Highly skilled and engaged staff

People working at OPC are passionate about privacy and dedicated to promoting it. We need to continue building and valuing a strong organisational culture that ensures our people feel engaged and valued.

Our people's capacity, capability and commitment are critical to our success as a modern regulator. People working at the Office are highly skilled privacy practitioners who give excellent advice to individuals seeking support as well as to government agencies, businesses and other organisations who want to improve their privacy practice. Over the next four years, our priorities will shift towards more proactive and outcome-focused work.

We invest in ongoing capability building with the following four outcomes:

- Model and embed inspired and cohesive people leadership throughout the organisation, harnessing improved engagement and organisational performance.
- Invest in training and development for our people to set them up for success in their new operating environment and support them in their professional development.
- Recruit people with expert skills who will support us on our journey, especially in the fields of compliance and business analytics/ data collection and analysis.
- Improve the office's understanding and use of Māori culture and language skills.

Effective strategic engagement with stakeholders

We are part of a wider privacy system and need to work with and through others to ensure we are as effective as we can be.

We cannot have all the information, experience or answers. Connecting with national and international regulators enables us to pool resources, share wisdom and practice, and to learn

from others. In addition, effective implementation of good privacy practices requires buy-in from others.

- We foster the open exchange of ideas with privacy professionals, public and private organisations, academics, communities and individuals.
- Our relationship management, communication and networking skills enable us to understand unique challenges in the privacy space and address them through channels that account for individual circumstances.
- We are good at interacting with associations and industry bodies that can distribute our messages as 'multipliers', and ensure we communicate our key messages effectively.

Meaningful performance measures

We want to improve individuals' privacy outcomes. In order to do that, we need an in-depth understanding of the effectiveness of our interventions. We will therefore collect insights and monitor our work against meaningful performance measures.

Our performance measures accurately capture how businesses and government agencies are doing in the privacy space, where the key challenges lie, and how well we are addressing these challenges.

These are the outcomes we will work towards:

- Our performance measures of each part of the Office align with our objectives and strategic priorities and identify critical performance indicators.
- Professional development practices enable people to have a clear direction on their role and how they contribute to the Office's success.
- Performance measures are reviewed regularly, and we continuously improve how we define, measure and report back on success.

Equal Employment Opportunities and Good Employer Statement

The Privacy Commissioner has an EEO policy and is an equal opportunities employer in its recruitment, human resources and staff development practices. The Privacy Commissioner has documented human resource policies and regularly reviews staff morale as part of management reporting.

We aim to provide equal employment opportunities to make the most of the talents of all our people. We assess our status as a good employer against the elements and criteria set out by the Human Rights Commission. Over the next four years we will continue to ensure that all elements are in place and working well.

The Privacy Commissioner reports on the Key Employment Elements in the Office through the Annual Report.