Privacy Commissioner
Te Mana Matapono Matatapu

# Privacy Impact Assessment on the use of Microsoft cloud services

# Review Report

**14 June 2023**

# Introduction

The Office of the Privacy Commissioner ("OPC") made the decision in 2018 to store its data in the cloud, using Infrastructure (IaaS), Platform (PaaS) and Software as a Service (SaaS) products as part of Microsft Azure and Microsoft 365 ("Microsoft solution"). At that time, we completed a full Privacy Impact Assessment ("PIA") on the move, which we updated in August 2019 to reflect changes to Australia's legal framework governing lawful requests for data.[1]

This is a review of our PIA, five years after we implemented the Microsoft solution. The reasons for this review are set out below. This review report should be read in conjunction with the 2018 PIA as updated in 2019 ("initial PIA"), which remains an important account of our initial risk assessment and due diligence processes.

# Our initial PIA

Following our full PIA process in 2018, we made the decision that, on balance, the Microsoft solution provided the best overall outcome for us, deliering to all our needs while reasonably protecting individual privacy. Specifically, we found that:

- The Microsoft solution best met our infrastructure requirements and effectlively addressed the system contraints we were experiencing at that time.
- Taking into account government policy, the law and a risk-based approach, the Microsoft solution remained the preferred and prudent option.
- Microsoft offered industry leading data security, and better data security than we were able to deliver at that time.
- We were comfortable that the regulatory framework in Australia – where our data would be stored at rest – provided a suitable level of protection (and we reviewed and reconfirmed this decision in 2019).
- The storage of our data in an offshore cloud solution involved a theoretical risk that an overseas government or law enforcement agency could make a request for our data. However, the likelihood of this occurring was extremely low.
- Adequate contractual and process controls were in place to ensure that any lawful requests would be redirected to us for consideration.
- The combination of assurances, contractual provisions, independent audits and certifications, and the applicability of local and overseas privacy regulations would effectively ensure that we had meaningful control over our data while it was stored in the cloud.

[1] The August 2019 PIA can be accessed at https://privacy.org.nz/assets/New-order/Resources-/Publications/Statements-and-media-releases/Updated-Public-Privacy-Impact-Assessment-Report.pdf.

- Making our PIA available, updating our privacy statement and taking steps to engage with any concerns would effectively ensure that we were as open and transparent as possible about our use of offshore public cloud services.

## Why we are conducting this review

PIAs should be living documents. This means that they should be periodically revisited to ensure that the decisions made in those risk assessments remain valid and to address any changes that might impact, for better or worse, on the overall privacy risk of a project.

We have decided to conduct this review for the following reasons in particular:

- To reflect on the findings we made in 2018 relating to the benefits of the Microsoft solution. It is important to ensure that those benefits have materialised, and that this solution continues to deliver to our needs.
- To accommodate privacy law changes introduced by the Privacy Act 2020 ("2020 Act"), to ensure that we have considered and addressed any new or altered obligations implemented by the reform.
- To assess whether, since 2019, there have been any developments in relation to the jurisdictional risk to our data by virtue of it being stored at rest in Australia.
- To consider and better articulate our response to cultural privacy perspectives on our decision to use an offshore public cloud service, including in relation to Māori data sovereignty.
- To identify and assess any internal changes to our business practices or processes that might impact on our risk profile or risk appetite.
- To identify and assess any changes to Microsoft's settings or contractual assurances that might impact, whether positively or negatively, on the privacy risk presented by the Microsoft solution.
- To ensure that we implemented all the controls and mitigations we identified as necessary in the initial PIA, such that we have effectively mitigated the risks.

## Our PIA is specific to our situation

Our PIA and this review report are specific to our situation. They reflect our risk profile and our risk appetite, the combination of which meant that we felt comfortable to use the Microsoft solution to store and process our data. It is not appropriate for other agencies to rely on our PIA as a justification to use the Microsoft solution, or any other cloud solution, to store and process their own data.

Agencies must make their own assessment and decision on such a move, taking into consideration their own risk profile – based on the personal information they hold, the nature of services they deliver, the expectations of their stakeholders and data subjects, and their security posture – and risk appetite. While agencies might wish to take a lead from the OPC, and could adopt a similar approach to assessing their privacy risk, it is critical that they undertake their own specific risk assessment.

## Performance of the solution

We have taken a risk-based approach to our assessment of the Microsoft solution. This required consideration of all relevant factors, including the benefits of a particular solution and, conversely, the risks of not adopting that solution. An important consideration therefore was whether the Microsoft solution delivered what we needed. As noted above, we decided that it did.

However, things can change. So, in addition to considering whether any of the risks have changed, this review must also consider whether the benefits we identified in our initial PIA materialised, and continue to be relevant, such that they should still influence our overall risk assessment. On reflection, and based on our actual use of the solution, it remains our view that the Microsoft solution best meets our infrastructure requirements and addresses our previous system constraints. In particular, the Microsoft solution continues to deliver the following benefits:

- It offers robust data protection and security capabilities.
- It is highly available and resilient. For example, it has protected us from denial-of-service attacks in a way an in-house solution could not.
- It is scalable and adaptable. For example, it has enabled us to add or remove requirements and integrations with ease.
- It offers industry standard business continuity and disaster recovery options.
- It is cost effective when compared to other options in the market.
- It ensures a consistent user experience.
- It supports secure flexible working, which was critical for us during the Covid-19 pandemic and continues to underpin our flexible working arrangements.

## Endorsement and refresh of Cloud First Policy

In the initial PIA, we noted that the government had adopted a Cloud First Policy, focused on accelerating the adoption of public cloud services by public sector agencies. On 4 April 2023, Cabinet endorsed the Cloud First Policy but also refreshed the policy to meet present day risks and considerations.[2] While reconfirming that the policy directs agencies to adopt public cloud services in preference to traditional ICT systems, Cabinet agreed that:

- Agencies should consider accountability, ethics, transparency and collaboration in relation to Māori data, when making decisions about adopting cloud services (see below at page 7).

[2] See https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/about/cabinet-minutes-papers/april-2023-refresh-cloud-first-and-strengthening/?source=rss#:~:text=April%202023%20%E2%80%94%20Cabinet%20endorsed%20the,New%20Zealand%2Dbased%20data%20centres.

- Over time, RESTRICTED information should be hosted in a New Zealand based data centre, where possible (see below at page 11).

# Legislative developments

The initial PIA was completed by reference to the Privacy Act 1993 ("1993 Act"). Since that time, the Privacy Act 2020 has commenced. While many of the obligations contained in the information privacy principles ("IPPs") remain unchanged, it is necessary to ensure that our references to certain provisions in the 1993 Act are reframed to refer to the 2020 Act, and that we have considered any new or altered obligations.

## Provisions related to the use of cloud services

On page 5 of the initial PIA, we outlined the relevant provisions relating to the use of service providers. These provisions have been carried over to the 2020 Act, with some minor differences.

- Section 3(4) of the 1993 Act stated that personal information held by a third party for the sole purpose of storing or processing it for the principal agency was deemed to be held by the principal agency. This provision is now contained in section 11 of the 2020 Act. Section 11(2) of the 2020 Act states that if an agency (A) holds information for or on behalf of another agency (B), and does not use or disclose the information for its own purposes, then the information is treated as being held by B, not A. Section 11(4) clarifies that this is the case whether A is outside New Zealand or holds the information outside New Zealand.
- IPP 5(b) of the 1993 Act stated that, if it was necessary to provide personal information to a service provider, the principal agency must do everything reasonably within its power to prevent the unauthorised use or disclosure of that information. IPP 5(b) of the 2020 Act carries over this provision essentially unchanged.
- Sections 10(1) and 10(2) of the 1993 Act made it clear that IPPs 5, 6, 7 and 8 to 11 applied to personal information transferred out of New Zealand. These specific provisions were not carried over to the 2020 Act. However, this is because the 2020 Act contains updated application provisions, at section 4, which include a clarification at section 4(2) that the Act applies to a New Zealand agency regardless of where the personal information is held by the agency. Thus, as we noted in the initial PIA, we remain subject to the IPPs despite the fact that we store and process our data outside New Zealand.

## Risk-based approach

On page 5 of the initial PIA, we noted that section 14(a) of the 1993 Act supported a risk-based approach, requiring the Privacy Commissioner to have regard to matters that may legitimately compete with privacy, including the general desirability of a free flow of information and the right of government and business to achieve their objectives in an efficient way.

Section 21(a) of the 2020 Act carries over this provision. It includes several minor stylistic changes that have no substantive importance. However, the introductory sentence of the provision has been altered in a way that recasts the obligation somewhat. Where section 14(b)

of the 1993 Act required the Commissioner to "have due regard for the protection of important human rights and social interests that compete with privacy", section 21(a) of the 2020 Act requires the Commissioner to "have regard to the privacy interests of individuals alongside other human rights and interests". The key difference is the removal of the word "compete" and the insertion of the word "alongside".

In our view, section 21(a) of the 2020 Act continues to support a risk-based approach to the management of personal information, but better reflects our long-held view that good privacy practice should not involve the balancing of competing interests, but rather the creation of solutions that deliver to all the interests at play, including privacy. Importantly, we believe that the Microsoft solution delivers such an outcome, and allows us to consider and address our system needs and constraints "alongside" the privacy interests of interests of individuals, with neither losing out.

## Changes to the existing IPPs

On pages 7-9 of the initial PIA, we summarised which of the IPPs we considered were specifically impacted by our move to the Microsoft solution. While some of these principles have been amended in the 2020 Act, none of these amendments alter our initial assessment.

- IPP 3 – Only minor stylistic changes were made to IPP 3, and our initial assessment of the impact of the Microsoft solution on this IPP remains valid.
- IPP 5 – Only minor stylistic changes were made to IPP 5, and our initial assessment of the impact of the Microsoft solution on this IPP remains valid. As noted above, IPP 5(b) still requires us to ensure that our service providers can protect the information they process on our behalf.
- IPP 9 - Only minor stylistic changes were made to IPP 9, and our initial assessment of the impact of the Microsoft solution on this IPP remains valid.
- IPP 10 – Only minor stylistic and structure changes were made to IPP 10 (including the re-ordering of some exceptions), and our initial assessment of the impact of the Microsoft solution on this IPP remains valid.
- IPP 11 - Only minor stylistic and structure changes were made to IPP 11 (including the re-ordering of some exceptions), and our initial assessment of the impact of the Microsoft solution on this IPP remains valid. However, IPP 11 was also amended to add reference to a new IPP 12, which is addressed below.

## IPP 12 – disclosing information outside New Zealand

A new IPP 12 was included in the 2020 Act, which relates to the disclosure of personal information outside New Zealand. In summary, IPP 12 states that an agency may only disclose personal information to a foreign person or entity if it can rely on one of the exceptions to do so. IPP 12 is intended to ensure that an agency remains accountable for the personal information it discloses outside New Zealand, on the basis that the information may no longer be protected by privacy laws equivalent to the 2020 Act.

However, IPP 12 does not apply to the transfer of personal information to a service provider. This is because such a transfer is not deemed to be a "disclosure" for the purposes of IPP 11.

Section 11(5) of the 2020 Act states that, where an agency (A) is storing or processing personal information solely on behalf of another agency (B):

- the transfer of the information to A by B is not a use or disclosure of the information by B; and
- the transfer of the information, and any information derived from the processing of that information, to B by A is not a use or disclosure of the information by A.

On this basis, for the purposes of our PIA in relation to the Microsoft solution and based on our contractual arrangement with Microsoft, we do not have to consider IPP 12. It is worth noting, however, that the exclusion of service provider transfers from the scope of IPP 12 does not leave data less protected. Such personal information will remain under the protection of the 2020 Act, because B (the OPC in this case) is subject to it. Further, as noted above, IPP 5(b) requires OPC to ensure that Microsoft will take reasonable steps to protect the information.

## Mandatory privacy breach notification

Part 6, subpart 1, of the 2020 Act introduced a mandatory requirement to notify serious privacy breaches. These provisions require an agency to notify both the Privacy Commissioner and generally the affected individuals of any privacy breach that has caused, or is likely to cause, serious harm to the affected individuals. Importantly, section 121(4) of the 2020 Act states that a principal agency is deemed to know about a breach as soon as its service provider knows about it. This means that we must be confident that Microsoft will promptly inform us of a privacy breach, so that we can manage that breach and meet our breach notification obligations in a timely manner.

In the initial PIA, we noted that the August 2018 version of Microsoft's Online Service Terms ("OST") provided a contractual assurance that Microsoft would promptly notify the customer of any security incident that affects its data, and would investigate the incident, provide the customer with detailed information about it and take steps to mitigate harm caused by it. The OST also stated that Microsoft would assist the customer to comply with any data breach notification laws.

Below, in the "Microsoft developments" section, we summarise our review of Microsoft's current Data Protection Addendum, and confirm that this assurance remains in place. In our view, this is sufficient to ensure that the Microsoft solution will not prevent us from meeting our privacy breach notification obligations.

## Taking cultural privacy perspectives into account

Section 21(c) of the 2020 Act has introduced a new obligation on the Privacy Commissioner to take account of cultural perspectives on privacy when performing their statutory functions. This change is an important recognition of New Zealand's bicultural foundations and reflects that the Privacy Act needs to be interpreted and applied in a way that is sensitive to different perspectives on privacy, and particularly indigenous perspectives.

This aligns with the OPC's recognition of the importance and relevance of the principles of Te Tiriti o Waitangi (the Treaty of Waitangi), and the concepts of partnership, participation and protection.[3]

For New Zealand, this manifests primarily in the concept of Māori data sovereignty ("MDS"). MDS refers to the inherent rights and interests that Māori have in relation to the collection, ownership, and application of Māori data, regardless of where it is processed or stored.[4] While broader than the issue of data location, MDS incorporates the principle that, whenever possible, Māori data should be stored in Aotearoa.[5]

As discussed in the initial PIA, we made the decision in 2018 – and reaffirmed in 2019 – to store our data at rest in Australia. This was a risk-based decision that took into consideration the location options available to us, the legal framework in Australia, and the contractual protections we had in place with Microsoft. In 2024, Microsoft will open a data centre in Aotearoa, and our intention is to move our data onshore as soon as this becomes possible.

We are committed to exploring further the ways in which we can meaningfully engage with Māori and better respond to and accommodate MDS in our own processes and settings, and we will continue to review our options in relation to the storage and control of our data. In the meantime, we believe that the onshoring of our primary data in due course, combined with the mechanisms in place to give us meaningful control of our data and manage the risk of overseas lawful requests, will take us in the right direction.

## Review of jurisdictional risk

As noted above, we intend to onshore our data when that option is available. However, in the meantime, our data will continue to be stored at rest in Australia and there is a possibility that we will continue to store a backup of our data in Australia. For this reason, we need to assess whether any developments in Australia since 2019 have altered the jurisdictional risk such that our decision on this risk should change.

In the initial PIA, we documented our assessment of the Australian Privacy Act, and formed the view that the Australian privacy regulatory framework was sufficient and provided an acceptable level of protection for our data. Since that time, the Australian Privacy Act has been undergoing a significant reform process. Much of the proposed reform is intended to strengthen the Act and remove several of the exemptions we noted in the initial PIA. While most of these reforms have yet to be finalised, the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 was passed in late 2022, and introduces significantly higher punitive fines for serious breaches of the Act – up to AU$50 million – and provides the Office of the Australian Information Commissioner with greater information sharing powers to better enforce the Act.

[3] Office of the Privacy Commissioner *Compliance and Regulatory Framework* November 2020, page 11.
[4] Te Kāhui Raraunga *Māori data sovereignty and offshoring of Māori data* July 2022, page 4; Te Kāhui Raraunga *Māori Data Governance Model* May 2023, page 37
[5] Te Mana Raraunga *Principles of Māori data sovereignty* 2018; Te Kāhui Raraunga *Māori Data Governance Model* May 2023.

There have also been some developments in relation to Australia's legal framework governing lawful requests for data. On 24 June 2021, the Telecommunications Legislation Amendment (Internal Production Orders) Act 2021 was passed. This legislation established a new international production orders framework under the Telecommunications (Interception and Access) Act 1979 which enables Commonwealth, state and territory agencies to seek data, via the Australian Designated Authority, from communications service provides in foreign countries with which Australia has a designated agreement. At the end of 2022, the first such agreement – the Australia-US Cloud Act Agreement – came into force. This agreement requires each country to lift restrictions that would otherwise inhibit their domestic providers complying with orders issued by the other country.

This means that cloud service providers headquartered in Australia – whether or not they have a US parent – could be subject to warrants under the US CLOUD Act. However, given that Microsoft is already subject to the US CLOUD Act by virtue of its US parent, these changes do not significantly alter the risk for us and our data. Further, our conclusion in the initial PIA – that the actual likelihood of our data being subject to lawful requests, whether from Australian or US authorities, was low – remains valid.[6]

In December 2021, the Parliamentary Joint Committee on Intelligence and Security published the report on its review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018.[7] In addition to reviewing the operation of the various new interception and information gathering powers enabled by the Act, chapter 7 of the report considered the sufficiency of the reporting and oversight mechanisms in place (which were an important factor in our initial assessment of jurisdictional risk). Noting that appropriate oversight and accountability mechanisms are critical in ensuring the public's ongoing confidence in the use of powers, the Committee made several recommendations to increase authorisation and oversight mechanisms, including by considering the establishment of a new Investigatory Powers Division of the Administrative Appeals Tribunal, and by requiring more transparency to the Committee on the use of certain powers. As far as we know, the Australian government has not yet responded to the recommendations. We will keep a watching brief on these developments.

We note that it was reported in 2020 that the Parliamentary Service had stalled a move to Microsoft 365 on the basis of the decryption law.[8] However, this decision was based on the Service's specific risk profile. The Service delivers communications, data and technology

[6] It should be noted that in Microsoft's latest Law Enforcement Requests Report (January-June 2022), it was reported that of 779 law enforcement requests relating to Australia, no requests resulted in the disclosure of content. See https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report.

[7] Parliament of the Commonwealth of Australia, Parliamentary Joint Committee on Intelligence and Security *Review of the amendments made by the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018,* December 2021. The full report can be found at https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024428/toc_pdf/ReviewoftheamendmentsmadebytheTelecommunicationsandOtherLegislationAmendment(AssistanceandAccess)Act2018.pdf;fileType=application%2Fpdf.

[8] https://www.reseller.co.nz/article/678599/australian-backdoor-law-forces-cloud-rethink-new-zealand-parliament.

infrastructure services to Parliament, the DPMC and a number of other government agencies within the parliamentary precinct. As part of this function, the Service must maintain parliamentary privilege and consider national security implications of exposing parliamentary communications to jurisdictional risk.

## Updates to Microsoft's contractual assurances

The initial PIA was completed on the basis of the contractual assurances we were given at the time, in both our contractual agreement with Microsoft and Microsoft's general OST. There have been no changes to our contractual agreement with Microsoft. However, the data protection terms in the OST has been revised several times since our initial PIA, and so we have reviewed the current version to ensure that it still contains the assurances we previously identified as necessary.

| August 2018 OST | Current Data Processing Addendum ("DPA")[9] |
|---|---|
| If compelled by law to disclose customer data, Microsoft will promptly notify the customer and provide a copy of the demand (unless prohibited by law from doing so). | Yes, and no material changes have been made to this assurance. |
| Microsoft will not give the law enforcement agency direct access to the data and will not give the agency the customer's cryptographic keys. | Yes, and no material changes have been made to this assurance. |
| Microsoft and its subprocessors will use customer data only to provide the services sought and will not use it for any commercial purposes (such as advertising). It also provides that the customer retains all right, title and interest in and to the data. | Yes, and no material changes have been made to this assurance. |
| Microsoft and its subprocessors will not disclose customer data unless the customer directs it to do so or as required by law. | Yes, and no material changes have been made to this assurance. |
| The customer may access, extract and delete its own data at any time. On termination of a service, Microsoft will retain any data still stored in the cloud for 90 days, after which time it is deleted. | Yes, and no material changes have been made to this assurance. |

[9] Microsoft has separated its Data Protection Terms from the OST, and now maintains a Data Processing Addendum ("DPA") that applies to all its products and services. The most recent version of the DPA is dated 1 January 2023, and can be found at https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.

| August 2018 OST | Current Data Processing Addendum ("DPA")[9] |
|---|---|
| Microsoft will promptly notify the customer of any security incident that affects its data, and will investigate the incident, provide the customer with detailed information about it and take steps to mitigate harm caused by it. The OST also states that Microsoft will assist the customer to comply with any data breach notification laws. | Yes, and no material changes have been made to this assurance. |
| Microsoft will conduct regular independent audits required to maintain its certification in a range of international compliance frameworks. | Yes, and no material changes have been made to this assurance. |

## Implementation of controls

An important step in any PIA process is to reflect on whether the risk mitigations identified in a PIA have been implemented and effective. In Appendix 1 of the initial PIA, we identified several controls intended to mitigate specific risks. We have addressed all of the mitigations and controls and, in some cases, have taken further steps to protect the data we store and process in the Microsoft solution.

| Risk ref | Mitigation | Action |
|---|---|---|
| **R-3.1** | Update OPC's enterprise-wide privacy statement to provide clear notice about the storage of personal information in the cloud. | Completed. |
| | Update all collection notices to link to this new privacy statement. | Completed. |
| | Make the PIA publicly available. | Completed. |
| **R-5.1**<br>**R-5.3** | Ensure Quantum Security recommendations and controls are implemented. | Completed where appropriate and necessary. |
| **R-5.3** | Create clear policy on the use of staff personal devices and remote access solutions. | Obsolete – OPC has now issued all staff with corporate laptops and must sign an attestation to confirm that they will not access OPC data on their own devices |
| | Develop data security training for staff once the new solution is implemented. | Completed, and delivered at induction<br>Complemented by ongoing security awareness. |

| Risk ref | Mitigation | Action |
|---|---|---|
| **R-5.6** | OPC policy will ensure that no documents security classified at CONFIDENTIAL and above will be processed or stored in its Microsoft cloud solution.[10] | Completed, and continuously applied. Government expectation is that over time RESTRICTED information should be hosted in a New Zealand based data centre, where possible. This expectation should be addressed by our intent to onshore our data. |
| **R-5.7** | Contractual obligations for the patching and maintenance of its IT infrastructure, network and software form part of OPC's current arrangements with LANWorx and will be extended for its Microsoft cloud solution. | Completed, and regularly reviewed by both LANWorx and OPC. |
| **R-10.1** | Request audit reports to substantiate assurances and contractual provisions. | Completed. |
| **R-11.1** | OPC should monitor any changes to the OST to ensure that the current assurances remain unchanged. | Completed, as evidenced in this review report. We will continue to review the OST and DPA periodically. |

## Conclusion

On the basis of this review report, we remain satisfied that, on balance, the Microsoft solution provides the best overall outcome for us, delivering to all our needs while reasonably protecting individual privacy. In summary:

- The Microsoft solution continues to best meet our infrastructure requirements and address our previous system constraints.
- Our use of the Microsoft solution complies with the relevant provisions of the 2020 Act.
- More work can be done to ensure we are properly engaging with Māori and responding to Māori data sovereignty considerations, including by onshoring our data in Aotearoa in due course, when this option becomes available in the short to medium term.
- The jurisdictional risk presented by storing our data in Australia remains acceptable to us, in view of the low likelihood of lawful requests for our data and the contractual assurances we have been given by Microsoft.
- The contractual assurances we relied upon in our initial PIA remain in place.

[10] This requirement has been reconfirmed by Cabinet as part of the endorsement of the Cloud First Policy, referred to above at n2. However, Cabinet has also stated that over time, RESTRICTED information should be hosted in a New Zealand based data centre, where possible.

- We have implemented all the mitigations and controls we identified as necessary in the initial PIA, and these have successfully protected our data for the preceding five years.

We will review our decision to use the Microsoft solution again when there is a significant internal or external change that might impact on our risk profile or our decision to use the solution – such as when we move to onshore our data in Aotearoa. In the absence of any other significant change, we have scheduled a regular five-yearly review cycle.