Privacy Commissioner
Te Mana Matapono Matatapu

Privacy Impact Assessment on the use of Microsoft cloud services

23 October 2018

Key messages

1	The Microsoft cloud solution best meets our infrastructure requirements and effectively addresses our current system constraints
2	Taking into account government policy, the law and a risk-based approach, the Microsoft cloud solution remains the preferred and prudent option
3	Microsoft offers industry leading data security, and better data security than we can currently deliver
4	We are comfortable that the regulatory framework in Australia is adequate and provides an equivalent level of protection
5	The storage of our data on an offshore cloud solution involves a theoretical risk that an overseas government or law enforcement agency could make a request for our data. However, the likelihood of this occurring is extremely low
6	Adequate contractual and process controls are in place to ensure that any lawful request will be redirected to us for consideration
7	The combination of assurances, contractual provisions, independent audits and certifications, and the applicability of local and overseas privacy regulations will effectively ensure that we have meaningful control over our data while it is stored in the cloud
8	Making this PIA available, updating our privacy statement and taking steps to engage with any concerns will effectively ensure that we are as open and transparent as possible about our use of offshore public cloud services
9	On balance, we are satisfied that the Microsoft solution provides the best overall outcome, delivering to all our needs while reasonably protecting individual privacy

Introduction

The Office of the Privacy Commissioner ("OPC") has made the decision 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 Office 365.

This privacy impact assessment ("PIA") explains the process we followed, the factors we considered, and the steps we have taken or are taking to make sure this decision does not adversely affect the privacy of New Zealanders. In making our PIA publicly available, we are seeking to ensure that our customers and stakeholders can have comfort that we have made a careful and safe decision about the way we will handle the personal information entrusted to us.

This PIA describes the journey we took to establish our confidence in moving to the cloud. It explains our reasons for the move, the context within which we made the decision, the key privacy risks we identified as potential barriers to cloud use, and the reasons we were satisfied they could be overcome.

The report, the process we followed, and our final decision on the move to the cloud reflect a risk-based approach to privacy practice. The Privacy Act contemplates that privacy must be one consideration among many for a public or private sector agency charged with delivering effective, efficient and responsible services. Of course, good services must not be delivered at the expense of individual privacy but, likewise, privacy should not be a barrier to innovation or transformation. This is a Privacy by Design approach, aimed at producing a positive sum outcome.

We have come to the conclusion that moving to the cloud provides us, and our customers, with significant benefits – including privacy and security benefits – and that the various controls available throughout the process mitigate any privacy risks that remain.

OPC's reasons for moving to the cloud

The OPC currently operates a traditional IT model, with on premise servers located in our Auckland office and a Remote Desktop Server ("RDS") that allows remote access. This infrastructure was last upgraded in 2012. At that time, we refreshed our systems with the intention that they would last for at least five years. Six years later, our systems are coming under increasing strain and our software and platforms are considerably out-of-date.

This has slowed and degraded the performance of our infrastructure, particularly for our Wellington office, which is affecting our ability to efficiently and effectively deliver our core services. Our current infrastructure suffers from the following key operational constraints:

- It is **not scalable**, which means we cannot readily increase the capacity of our infrastructure as we grow.
- It has **limited durability**, which creates data integrity risks for us.

- It offers **limited business continuity or disaster recovery options**, which could impact our ability to deliver ongoing services.
- It is **costly** to operate and maintain, which restricts our capacity to grow and drive other privacy initiatives.
- It provides **inconsistent user experience**, which can create confusion about the cause of system issues.
- It focuses on delivering **physical data security**, which limits our flexibility and could expose us to other security risks.
- It **does not support flexible working**, due to limitations in remote access options.

We considered a number of options to upgrade our infrastructure to address the above constraints. We reviewed the feasibility of continued on premise (our own servers located in our own offices), co-location (our own servers located somewhere else), onshore cloud, offshore cloud, or hybrid solutions.

On balance, we have found that the offshore cloud option, and particularly the Microsoft solution, best meets our infrastructure requirements, including data security, business continuity, disaster recovery, scalability, cost, user experience, availability and resilience. We believe that by effectively addressing the constraints outlined above, this solution provides significant benefits for our employees, our customers and our stakeholders.

The Microsoft cloud solution best meets our infrastructure requirements and effectively addresses our current system constraints

Context and environment

Cloud technology and services have advanced rapidly in recent years, such that they offer industry best practice productivity, data storage and data processing services at a fraction of the cost of traditional IT systems. Public cloud services have become a mainstream technology choice for private sector agencies worldwide, with data security cited as a major reason for this choice. In short, the world is moving to the cloud and the reasons not to are fast diminishing.

Government's cloud first policy

The political appetite for cloud services has also evolved, with the previous government's adoption of a "cloud first" policy. The 2015 *Government ICT Strategy* required public sector agencies to "adopt cloud services in preference to traditional IT systems because they are most cost effective, agile, and generally more secure, and provide greater choice".

In 2016, the government released a cabinet paper, *Accelerating the Adoption of Public Cloud Services*, which aimed to further this policy by setting a range of measures to accelerate the adoption of public cloud services by public sector agencies. As part of this, the government removed a previous restriction on the use of offshore cloud productivity

services. It was recognised that this restriction sent a message to agencies that public cloud services were too high risk.

Today, the government supports a careful, risk-based adoption of public cloud services, provided appropriate safeguards are put in place. Both the government's cloud first policy and the various guidance it has released have informed our considerations of the privacy and security implications of adopting the Microsoft solution. Our ability to comply with the government's security requirements for offshore cloud services is summarised further below.

The Privacy Act

The Privacy Act 1993 does not prohibit the use of cloud services, whether within New Zealand or offshore. In fact, it anticipates that agencies may use the services of third parties to process or store their data and may send that data outside New Zealand for such purposes. Rather, the Act focuses on ensuring accountability in the use of cloud services:

- Section 3(4) of the Act states that personal information held by a third party for the sole purpose of storing or processing it for the principal agency is deemed to be held by the principal agency. In other words the principal agency remains liable and accountable for the personal information it stores or processes within a cloud service.
- Principle 5(2) of the Act states that, if it is necessary to provide personal information to a third party, the principal agency must do everything reasonably within its power to prevent unauthorised use or disclosure of that information. Again, therefore, the principal agency remains liable and accountable for the protection of its personal information.
- Finally, section 10 of the Act makes it clear that privacy principles 5, 6, 7 and 8 to 11 apply to personal information transferred out of New Zealand. This means that a principal agency remains directly subject to the relevant privacy principles, and so it must take additional care to ensure that it retains control over its data.

Further, the Privacy Bill currently making its way through the legislative process contemplates new restrictions on transferring personal information out of New Zealand. While the current drafting would exempt from these restrictions personal information being transferred for the purposes of utilising cloud services, it does raise issues in respect of the possible disclosure of personal information to offshore third parties by a cloud service provider. For this reason, jurisdictional issues and the risk of law enforcement requests are a consideration in this PIA.

Risk-based approach

The legal framework outlined above is not the whole story however. The Privacy Act also expressly allows for a risk-based approach to the management of personal information that recognises privacy is one of a number of important goals for any agency.

Section 14(a) of the Act requires the Privacy Commissioner to take into account a number of matters that may legitimately compete with privacy, including the general desirability of a free flow of information and the right of government (including the OPC) and business to achieve their objectives in an efficient way. Not doing this properly, with the result that the OPC is unable to deliver effective public services, is also a real risk that we must consider.

The government has expressly endorsed a risk-based approach too, stating in its *Government ICT Strategy* that, "[a]lthough it is important that the right balance is struck between innovation, security, and privacy, the clear focus will be on innovation and managed risk-taking that will deliver the public services expected by citizens".

A risk-based approach recognises that there is no one-size-fits-all approach to compliance with the Privacy Act, including the selection and use of cloud services. It requires a consideration of all relevant factors, including the type and sensitivity of personal information involved, the expectations of key stakeholders (including government), the other benefits of a particular solution (and, conversely, the risks of not adopting that solution), and the key privacy risks that must be understood.

What this means for us

We have already outlined above the benefits the Microsoft solution can deliver, which are significant in view of the expectation that we must deliver effective services to all New Zealanders within our budgetary constraints. A risk-based approach also required us to consider the risks that remained if we chose other options. We found that neither onshore cloud nor traditional on premise solutions addressed our key constraints as effectively as the offshore cloud solution, but both still presented privacy risks that we would have to overcome.

For example, our on premise solution would be less secure from a physical and system perspective. An onshore cloud solution would still be subject to the control issues considered later in this PIA. While both the on premise and onshore cloud solutions may have addressed some jurisdictional risks, we had to balance this against the reality that Microsoft was able to deliver a level of physical, system and process security that surpassed the other options available to us.

Taking into account government policy, the law and a risk-based approach, the Microsoft cloud solution remains the preferred and prudent option

Our preferred solution and the information flows

Personal information involved

OPC collects a significant amount of personal information as part of its core functions. This information ranges from the more trivial (such as contact or administrative information about a complainant) to the highly sensitive (such as health information or information about criminal investigations or prosecutions).

We also generate personal information, for example when we discuss, communicate about or form opinions on complaints or other matters that relate to individuals. Finally, as with any employer, we collect and generate personal information about our employees.

We will store and process within the Microsoft solution the personal information we collect and hold, with the exception of any government information security classified as

CONFIDENTIAL or higher (which we rarely collect or hold but, if we do, we will store and process separately).

As the OPC carries out the majority of its work by email (including the sharing of information or documents with complainants and respondents and the delivery of legal views on complaints), most of the personal information we collect and hold will be processed within both Azure and Office 365 services and applications. This includes our document management system and our use of the Microsoft Office suite of applications for office productivity.

Data transit, storage and processing

All the Azure Core Services and Office 365 Services will be restricted to the geographic region of Australia. This means that all OPC data **at rest** will be stored in data centres within Australia, unless a major data centre disaster requires it to be transferred to another region.

We are satisfied that, whilst as part of delivering its cloud services, some encrypted OPC data will be transferred to or through, and may be temporarily stored in, other regions Microsoft or its subprocessors operate (including the United States) it will be on the following basis:

- **Azure Core Services** – no personal information will be transferred out of Australia, though some OPC enterprise metadata (such as security reports, user access data, or device data) may be.
- **Office 365 Services** – any data in transit may be transferred globally for the purpose of delivering services. Microsoft states: "When we move your data within our global systems and facilities for efficient processing, we implement robust policies and processes to protect it. We encrypt your data in transit, limit unauthorized access and use (even by Microsoft personnel), and avoid unauthorized storage of core customer data outside of [Australia]".[1]

Key privacy risks

Relevant privacy principles

The use of offshore cloud services does not change many of our privacy practices. It does not require us to collect new personal information from different sources. We will not be using personal information in new ways or intentionally disclosing it to any new agencies. However, the fact that we are asking another agency to store and process our data does require us to relinquish some control and this raises particular risks that must be considered.

The table below outlines what we consider to be the key privacy principles our IT upgrade impacts upon. Our full Privacy Risk and Mitigation Table is attached at appendix 1 below.

[1] It should be noted that the use of SEEMail affects the encryption of some email in transit. However, this is a current risk, and not one that has been created or exacerbated by the use of offshore cloud services.

Principle (in summary)	Relevance
Principle 3 **Be open with people about the personal information you collect**	People decide to share personal information with us when they make complaints or otherwise interact with us. Their trust in us as a data custodian will form a part of this willingness to share and we want people to ensure that they have a good reason to trust us and are not simply assuming we will protect their data because we are the regulator. We have made the decision that it is safe to store the personal information we hold in the cloud, but our customers cannot make an informed decision about sharing their information with us if they do not know where we store it. If we failed to be open with people about our use of cloud services, we would be at risk of real reputational damage. We need to lead by example. See *Openness and transparency* below.
Principle 5 **Take reasonable steps to protect personal information from harm**	We are entrusting our data to a third party and this requires us to transfer the data to the cloud and to data centres in other countries. This means that data protection is a key risk for us – while data is in transit and at rest – and we must ensure that using Microsoft services does not put our data at any more risk of harm. The government has made clear its expectations in relation to the secure use of cloud services. These expectations have formed part of our considerations of principle 5. A failure to ensure that our data was secure could cause harm to our data subjects and could significantly impact our reputation. See *Data security* below.
Principle 9 **Keep personal information only for as long as you need it**	This retention limitation is a critical part of data minimisation. We must ensure that we retain personal information for no longer than we have a lawful purpose to use it. By relinquishing some control of our data to a cloud provider, we may put our ability to comply with this principle at risk. A failure to ensure that our data was not retained for longer than we needed it could put us in breach of principle 9 and could expose our data, and our data subjects, to harm. See *Control and compliance* below.
Principle 10 **Use personal information only in the ways you said you would**	Compliance with this use limitation principle is at the heart of trust and reputation. The people we deal with need to have confidence that we will use their personal information only to meet our legislative purposes and will take steps to ensure that it is not used in other ways that could cause harm. By permitting other agencies, including Microsoft and its subprocessors, to store our data, we could be exposing the data to an increased risk of misuse. We need to be satisfied that this risk is effectively addressed. A failure to ensure that our data is not used by third parties for purposes that do not support our own could cause harm to our

Principle (in summary)	Relevance
	data subjects and could significantly impact our reputation. See *Control and compliance* below.
Principle 11 **Don't disclose personal information unless you really need to**	When we share our data with our cloud provider for storage or processing on our behalf, we are not disclosing it for the purposes of principle 11. The Privacy Act deems that information to be held by us. However, as with the use limitation issue above, we are exposing the data to an increased risk of disclosure by a third party. A key risk here is the disclosure of our data by Microsoft in response to a lawful request from a government or law enforcement agency in another country. We relinquish some control over this process by entrusting our data to Microsoft and so we must have confidence that it will manage these requests robustly. A failure to ensure that our data is protected from disclosure by third parties could cause harm to our data subjects, could significantly impact on our reputation and could also impact on the interests of the NZ government. See *Data sovereignty* and *Control and compliance* below.

Data security

Not surprisingly, data security is a key focus for this office, and for the government more widely. While it is expected that public sector agencies will move to the public cloud, they must do so in a considered way that ensures the security of government information, including personal information, is not compromised. The Government Chief Digital Officer ("GCDO") has provided guidance on assessing and managing data security risks in the cloud.[2] We have considered and applied this guidance and ensured that our use of Microsoft Azure meets government requirements.

Microsoft has also put significant effort into demonstrating its compliance with GCDO requirements. It has provided its own responses to the GCDO risk assessment questionnaires,[3] issued guides on Azure's[4] and Office 365's[5] conformance with the GCDO's security requirements, and published risk assessments, security certificates and independent audit reports on Office 365 and Azure services.[6] It also complies with a number of international compliance standards, including ISO 27001, 27002 and 27018.

[2] We have considered and applied: *Security Requirements for Offshore Hosted Office Productivity Services Explained* 19 January 2017, *Cloud Computing: Information Security and Privacy Considerations* April 2014, and the GCDO's *Cloud Risk Assessment Tool*.
[3] http://download.microsoft.com/download/3/3/1/33120588-5D1D-46E3-90EC-BDB2C272598B/Response%20to%20GCIO%20104%20questions%20-%20Microsoft%20Azure%20-%20release%20v5_17%20Mar%202015_FINAL.pdf
[4] https://aka.ms/azurecompliancenewzealand
[5] https://aka.ms/o365-gcio-conformance-guidance
[6] https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/design-for-and-implement-security-controls-for-cloud-services/

However, to ensure that we could be confident our data would be secure, we also obtained an independent security assessment, which assessed the Microsoft solution against our specific requirements and risks, including our need to comply with the government's security requirements. This assessment revealed a number of manageable security risks (some of which relate not to the solution itself but the safeguards we must put in place, including in respect of password management and OPC device protection) and provided us with a set of clear and practical controls to minimise or eliminate them.[7] We will ensure that all these controls are implemented.

Microsoft offers industry leading data security, and better data security than we can currently deliver

Jurisdictional risk

Storing personal information in servers located overseas can raise jurisdictional risks. As noted above, the Privacy Act permits agencies to send personal information overseas for storage and processing. However, the Act seeks to address jurisdictional risk by expressly providing that liability and accountability for the data remains with the principal agency in New Zealand.

We have decided that Microsoft provides us with the best solution for reasons outlined above. This requires us to send our data offshore because Microsoft does not have data centres in New Zealand. Microsoft allows its customers to restrict the locations where its data at rest will be stored. We have chosen to restrict our data to data centres in Australia. As explained below, this ensures that our data at rest will be subject to the protection of laws that are equivalent to our own.

Privacy and legal framework in Australia

A cloud service provider based in Australia will be subject to the Privacy Act 1988 (Cth). This Act is substantially similar to New Zealand's Privacy Act. Both laws have common roots in the OECD Privacy Guidelines and the drafting of New Zealand's Act was based on the Australian Act.

The Australian Act applies substantive obligations to entities through a set of 'Australian Privacy Principles' (APPs) that cover much the same ground to the New Zealand information privacy principles. In some areas the Australian Act applies more stringent requirements, such as mandatory breach notification and the obligation on processors to make a written record of any lawful access to customer records.

Unlike the New Zealand Act, the Australian Act has not yet been given "EU adequacy". This is not because of any substantive deficiencies in the standards of the law itself (which has not formally been assessed) but because of a preliminary question of coverage. The EU was concerned at the breadth of two exemptions that were incompatible with a finding of adequacy. The first is a small business exemption that is irrelevant to Microsoft. The second is the exemption for employment records.

[7] One key risk relates to the management of cryptographic keys and this is discussed further below.

The Australian Act contains no equivalent to section 3(4) of the New Zealand Act (outlined above). Under the Australian Act, the third party provider and the principal agency appear to have equal liability and obligation under the law. This means the third party provider must take equal care to ensure compliance with the law (as it cannot transfer responsibility to its customer, the principal agency). While it may also have implications in respect of data control, we are satisfied that the contractual assurances Microsoft has provided to us (outlined below) adequately mitigate these.

We are comfortable that the regulatory framework in Australia is adequate and provides an equivalent level of protection

Lawful requests and Microsoft's process for responding to them

Lawful requests are requests made by a government, law enforcement or national security or intelligence agency under law, whether that is a court order (such as a search warrant or computer access warrant) or a legislative provision, for information that is being stored or processed within their territory. In theory, our data could be the subject of lawful requests, both from within New Zealand or from overseas under international agreements for law enforcement cooperation, if we chose an onshore cloud solution. However, the use of an offshore cloud solution does slightly increase the likelihood of our data being subject to overseas law enforcement requests.

Australia's legislative framework governing lawful access under search warrants or by national security agencies (the Australian Crimes Act 1914 and Australian Security Intelligence Organisation Act 1979) is broadly similar to that in New Zealand. In short, Australian law enforcement agencies may be able to request information for legitimate reasons but are subject to similar due process and oversight requirements to New Zealand agencies.

Microsoft has taken a transparent approach to lawful requests, and publishes a regular Law Enforcement Request Report,[8] which outlines the number of requests it has received by country. Its latest report showed that Microsoft received 824 law enforcement requests within Australia during the period July-December 2017. However, the report states that *none* of these requests resulted in the disclosure of content (as opposed to subscriber data). In fact, Microsoft reports that there has been no disclosure of content in the last five years.

There is also a low risk that overseas governments try to lawfully access information stored outside their territory by a cloud provider based within their territory. For example, the United States recently passed the US CLOUD Act, which asserts that US warrants have extra-territorial effect (though it does also provide a US-based cloud provider with the ability to challenge this on the basis that it creates a conflict with local law). Microsoft has taken an active role in ensuring that the US CLOUD Act is applied in a way that impacts to the least possible extent on its customers.[9]

[8] https://www.microsoft.com/en-us/about/corporate-responsibility/lerr

[9] See for example this blog by Microsoft President Brad Smith - https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/.

The actual likelihood of our data being subject to lawful requests, whether from Australian or US authorities, is low. We do not currently receive lawful requests from New Zealand authorities and there is no evidence to suggest that the mere storage of our data in Australia or any other overseas country would lead to lawful requests from overseas authorities.

The storage of our data on an offshore cloud solution involves a theoretical risk that an overseas government or law enforcement agency could make a request for our data. However, the likelihood of this occurring is extremely low

That said, by using a third party to store our data, we lose some control over the way any lawful requests are handled. For this reason, we need to have confidence in Microsoft's approach to all lawful requests, regardless of their source. In particular, we need to be confident that Microsoft will redirect requests for our data to us for consideration.

In its Online Services Terms ("OST"),[10] which are discussed further below, Microsoft makes a number of important contractual promises in respect of lawful requests, including:

- Microsoft will not disclose customer data to law enforcement unless required by law.
- Microsoft will attempt to redirect the request to the customer.
- 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).
- Microsoft will not give the law enforcement agency direct access to the data and will not give the agency the customer's cryptographic keys.

The circumstances in which Microsoft might be prohibited by law from notifying us about a lawful request are limited. The Australian Security Intelligence Organisation Act provides for secrecy in respect of the execution of search warrants or computer access warrants by intelligence agencies. US law provides a process under which prosecutors and investigators may prohibit a service provider from notifying the target of a lawful request if they can establish a risk to the investigation as a result, though such orders must be limited in duration.

We had discussions with Microsoft New Zealand as part of our PIA process. We were satisfied that Microsoft's process for managing lawful requests was robust. In practice, even where a lawful request prohibits notification, Microsoft stated that it would generally work with the requesting agency to identify someone within the customer agency who can be notified without compromising the investigation that prompted the request.

Finally, we note that Microsoft has publicly challenged lawful requests, with one case relating to a US warrant for the production of data held in its Irish data centre being challenged as far

[10] Microsoft Volume Licensing Online Services Terms (Worldwide, English, August 2018).

as the US Supreme Court (a case in which we filed a submission).[11] This provides some support for the assurances Microsoft makes about lawful requests.

Adequate contractual and process controls are in place to ensure that any lawful request will be redirected to us for consideration

Control and compliance

We recognise that, as the principal agency, we remain liable for the personal information we entrust to a third party cloud provider. This accountability is critical to the proper protection of personal information about New Zealanders, and this is so whether we choose to store the information here in New Zealand or overseas.

For this reason, it is important that we retain control over the personal information we store in the cloud, not least so that we can ensure that we are able to remain compliant with our obligations under the Privacy Act. This ability to meaningfully and practically control our data determines our ability to properly mitigate the risks outlined above, in respect of the security and retention of our information, and limitations on the access, use or disclosure of that information by Microsoft or its subprocessors.

To satisfy ourselves that we will truly retain control of the personal information we are storing in the cloud, we wanted to know what Microsoft's view was on these issues, what it was willing to promise to us in its contracts and agreements, and how independent auditors found Microsoft was living up to its promises. It was the combination of these elements that left us satisfied that we had adequate control over our data.

Control of cryptographic keys

A cryptographic key is a code that facilitates the encryption and decryption of data held in the cloud. Most of the data processing services which make the public cloud such an effective option rely on the cloud provider having access to the cryptographic key to process the data. This requires us to relinquish some control over our data.

We worked hard to understand the consequences of this and make the right decision on it, and took advice from independent experts, including security consultants. There are different options for managing the cryptographic key issue, and each has benefits and drawbacks.

Options that would allow us to generate, store and manage our own key provide the highest level of privacy protection but would be costly, require capabilities we do not have, and would break the very functionality we are looking to obtain from moving to the cloud. They would also create significant risk of permanent data loss if we or our agent were to lose the key.

By contrast, under Microsoft's default approach to key management, Microsoft would generate, store and manage the key on our behalf in accordance with its Security Policy. This option addresses the major drawbacks of storing and managing our own key. The cloud

[11] https://www.privacy.org.nz/news-and-publications/statements-media-releases/us-vs-microsoft-executing-search-warrants-across-borders/

functionality would be preserved, the cost would be greatly reduced and we would eliminate the risk of permanent data loss.

On balance, taking into consideration all of our risks, and in view of the other compensating controls (outlined below), we have opted to use Microsoft's default approach.

Assurances and contracts – Saying the right things

Microsoft makes a number of important contractual commitments designed to both assure and ensure that it will protect the data it processes on behalf of its customers.

As a first step, we will ensure that our contract with Microsoft protects our interests and the interests of our data subjects, preserving our position and the application of New Zealand law to any contractual disputes. However, we are also satisfied with the promises Microsoft has made in its generic Online Services Terms (OST), which we believe contribute to addressing the privacy risks we have identified:

- **Use of personal information** – The OST states that 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.
- **Disclosure of personal information** – The OST states that Microsoft and its subprocessors will not disclosure customer data unless the customer directs it to do so or as required by law. The OST also sets out clear commitments by Microsoft to manage lawful requests openly and robustly, and we have discussed this above.
- **Retention and deletion of personal information** – The OST states that 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.
- **Notification of data breaches** – The OST states that 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.

We also note that Microsoft has made a commitment to apply the EU Standard Contractual Clauses to all cloud services it applies. These clauses have been drafted to promote compliance with the more prescriptive EU General Data Protection Regulation. These clauses provide further contractual commitment in respect of breach notification, the use of subprocessors and the deletion of customer data.

Independent audit and certification – Doing the right things

Microsoft commits in its OST to conducting regular independent audits required to maintain its certification in a range of international compliance frameworks. Microsoft makes these audits available online. Microsoft complies with, for example, ISO 27001, ISO 27002, ISO 27018, SOC 1 and SOC 2. Many of these standards require regular auditing and independent verification to ensure that strict controls are being met.

Compliance with these independent standards and frameworks provides us with some independent assurance and verification that Microsoft is capable of delivering on its privacy and security promises.

The combination of assurances, contractual provisions, independent audits and certifications, and the applicability of local and overseas privacy regulations will effectively ensure that we have meaningful control over our data while it is stored in the cloud

Openness and transparency

We are comfortable that storing and processing our data within Microsoft's offshore cloud is safe and effective and does not put the personal information we hold at undue risk. However, we want our customers and stakeholders to know we are doing this and to understand why we have made this decision.

We are required by principle 3 of the Privacy Act to be open about the way we manage personal information. However, we also think it is simply the right thing to do. Transparency of this sort is a fundamental part of accountability, and we want to ensure that we are leading by example here. We also believe that being as open as we can be about our decision to use offshore cloud services will assist anyone with sensitivities about offshore cloud use to feel as reassured as we do that this will not put them at undue risk of harm.

To meet our openness and transparency obligations, we:

- have made this PIA public;
- have updated our privacy statement to include clear notice about our use of Microsoft services and the locations of our data;
- have updated our collection notices (such as the notice provided on our complaint form) to highlight this important change in practice and provide a link to our privacy statement; and
- will engage where required and appropriate with anyone who has particular concerns with our use of offshore cloud services.

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

Conclusion

We have taken a risk-based approach to the adoption of cloud services. In doing so, we have taken into account our obligations to deliver a set of important statutory functions efficiently and effectively, to spend public money wisely and with care, to prepare for the growth of our office and functions as a result of privacy law reform, and to ensure that we could meet all these goals in a way that reasonably protected individual privacy.

Having considered a number of options for upgrading our IT infrastructure, we have found that the Microsoft solution best meets our needs, in the most cost-effective way, while providing strong privacy and security protections.

We believe that Microsoft has more than adequately assured and demonstrated compliance with our privacy expectations as a New Zealand agency. With the additional safeguards outlined in this PIA in place, we think that the personal information we hold will be better protected than it is today, and we will be in a stronger position to meet the growing needs of our customers and stakeholders.

On balance, we are satisfied that the Microsoft solution provides the best overall outcome, delivering to all our needs while reasonably protecting individual privacy

Appendix 1: Privacy Risk and Mitigation Table

OPC Proposal to use Microsoft Offshore Cloud Services

Principle 1 : Purpose of collection of personal information

Ref. no.	Purpose of collecting the information	Description of the risk	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual current risk	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-1.1	OPC collects personal information which is necessary for the purpose of fulfilling its statutory functions and activities, including its function as an employer (section 13 Privacy Act).	Move to Azure does not impact on compliance with principle 1.	N/A	N/A	N/A	N/A	N/A

Principle 2: Source of personal information

Ref. no.	Source of personal information	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual current risk	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-2.1	OPC must collect personal information directly from the individuals concerned unless one of the IPP2 exceptions applies.	Move to Azure does not impact on compliance with principle 2.	N/A	N/A	N/A	N/A	N/A

Principle 3: Collection of personal information from the subject

Ref. no.	Telling the individual what you're doing	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual current risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-3.1	OPC must provide notice to its customers and employees about the personal information it collects, including how it will be processed and where it will be stored.	OPC fails to provide its customers or employees with notice about the storage and processing of personal information on an offshore cloud platform.	A failure to provide clear privacy notice about the use of offshore cloud services could put OPC in breach of principle 3. This lack of transparency could also impact OPC's reputation as a privacy leader.	OPC privacy notices and statements do not currently advise that personal information will be held in the cloud.	Significant	Update OPC's enterprise-wide privacy statement to provide clear notice about the storage of personal information in the cloud. Update all collection notices to link to this new privacy statement. Make this PIA publicly available.	Minimal

Principle 4: Manner of collection of personal information

Ref. no.	How you are collecting personal information	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-4.1	OPC must not collect personal information in ways that are unlawful or, in the circumstances, unfair or unreasonably intrusive.	Move to Azure does not impact on compliance with principle 4.	N/A	N/A	N/A	N/A	N/A

Principle 5: Storage and Security of personal information

Ref. no.	How you are storing and securing personal information	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-5.1	**Safe systems:** The software, platform and infrastructure OPC moves to as part of the Azure solution must provide adequate system and technical security to protect OPC data from harm.	The Microsoft Azure solution does not provide adequate system and technical security safeguards.	Inadequate system security safeguards could result in unauthorized access to and use or disclosure of OPC data. This would put OPC in breach of principle 5 and cause harm to OPC customer or employees or to OPC's reputation.	Microsoft Azure offers very comprehensive infrastructure, network, and data security features, including strong encryption in transit and at rest, penetration testing, DDoS protection etc. In its Online Services Terms ("OST"), Microsoft promises to provide technical and organizational security measures that comply with relevant ISO standards. Quantum Security has conducted a full security assessment of OPC's use of the Microsoft Azure solution. This assessment has recommended a number of controls, all of which will be implemented by OPC.	Minor	Ensure Quantum Security recommendations and controls are implemented.	Minimal

Ref. no.	How you are storing and securing personal information	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-5.2	**Safe places:** The data centres used by Microsoft to store OPC data must provide adequate physical security to protect OPC data from harm.	The Microsoft data centres do not provide adequate physical security safeguards.	Inadequate physical security safeguards could result in unauthorized access to and use or disclosure of OPC data, or the loss of OPC data. This would put OPC in breach of principle 5 and cause harm to OPC customer or employees or to OPC's reputation. This could also impact on OPC's ability to deliver services.	Microsoft data centres can provide more effective physical protection than OPC itself can guarantee onsite.	Minimal	N/A	Minimal
R-5.3	**Safe people:** OPC staff must understand how to access and use the Microsoft Azure solution safely, and ensure that their actions do not impact on otherwise secure systems.	OPC staff do not understand how to use the Microsoft Azure solution safely – whether by misusing or sharing passwords or using unsafe devices or networks.	A failure to ensure strong processes are in place to manage any security risks created by staff use of new services or software (including the potential for web access to OPC systems from personal devices) could reduce otherwise strong security safeguards. This could put OPC in breach of principle 5.	Microsoft provides strong user verification and access controls, including password protection and two factor authentication. Microsoft also provides access monitoring and logging to assist customers to manage this risk proactively. The Quantum Security report provides additional controls.	Significant	Ensure Quantum Security recommendations and controls are implemented. Create clear policy on the use of staff personal devices and remote access solutions. Develop data security training for staff once the new solution is implemented.	Minor

Ref. no.	How you are storing and securing personal information	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-5.4	**Safe jurisdictions:** The data centres used by Microsoft to store OPC data must be located in jurisdictions with equivalent privacy regulations to those in NZ.	The Microsoft datacenters are located in jurisdictions that do not have equivalent privacy regulations, so that OPC data is not protected sufficiently by law, which puts OPC.	Storing OPC data in jurisdictions will little or no privacy regulation could mean less protections are required and could impact on the ability for OPC or its customers to seek redress if there is a data breach or other incident.	Microsoft provides customers with the ability to choose the geographic region in which their data will be stored at rest. OPC intends to specify that its data be stored only in Australia (Sydney and Melbourne).	Minor	Microsoft will make available an updated list of its subprocessors and their locations. Microsoft is regularly audited against ISO standards in respect of the actions of their subprocessors. If we have concerns about a particular subprocessor, we can request a copy of the relevant audit report. If Microsoft uses a new subprocessor that stores OPC data in a third country with lesser privacy regulations in place, OPC may cancel the affected services (though in reality this is not a practicable control).	Minimal
R-5.5	OPC must be made aware of any data breaches or security incidents that may impact on its data and put its customers or employees at risk of harm.	Microsoft does not advise OPC of a data breach or security incident that may impact on its data.	OPC is unaware of risks to its data and therefore its customers or employees. OPC is prevented from meeting its data breach notification obligations to its customers, which relates in further individual harm.	In its OST, Microsoft promises to promptly notify the customer of any security incident affecting its data. Microsoft is also subject to the data breach notification scheme under the Australian Privacy Act, which also requires it (as data processor) to notify the affected customer (OPC).	Minimal	N/A	Minimal

Ref. no.	How you are storing/ securing personal information	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-5.6	Information, data or materials security classified at CONFIDENTIAL and above must not be stored or processed in OPC's cloud services.	Risk that information security classified as CONFIDENTIAL or above is stored off-shore, contrary to Cabinet direction.	Risk of significant reputational harm to OPC and to NZ government if information security classified as CONFIDENTIAL or above is stored offshore.	OPC complies with NZISM protective security requirements. OPC also ensures that its practices are consistent with other agency choices about cloud use. In addition, its use of SEEMail ensures that OPC can receive email only information security classified no higher than Sensitive or In Confidence. OPC's subscription to SEEMail does not allow transmission of documents security classified as "Restricted" or higher.	Minor	OPC policy will ensure that no documents security classified at CONFIDENTIAL and above will be processed or store in its Microsoft cloud solution. OPC will advise providers of information security classified as higher than Restricted to review the classification of the information to ensure OPC can process and store the information in its Microsoft cloud solution. OPC to amend its Procedures Manual to reiterate agencies' obligation to ensure that OPC is able to receive, process and store the information. Preferred approach is to review such material offsite at the agency concerned.	Minimal

Ref. no.	How you are storing and securing personal information	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-5.7	OPC must ensure that Microsoft security safeguards are complemented by OPC device management controls.	Insecure practices such as not applying security patches could result in an exploitable vulnerability.	A failure to ensure that OPC devices are patched and protected could result in unauthorized access to and use or disclosure of OPC data. This would put OPC in breach of principle 5 and cause harm to OPC customers or employees or to OPC's reputation.	OPC has contracted with its IT provider LANWorx to ensure that security patches are applied as required and its systems are appropriately maintained.	Significant	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. The consumption of some Microsoft services as PaaS or SaaS provides added assurance these activities are routinely undertaken.	Moderate

Ref. no.	How you are storing and securing personal information	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-5.8	Information will be stored in a multi-tenanted environment within the Microsoft Azure solution.	OPC information could be intermingled on the shared platform, compromising its security.	A failure to properly separate and protect OPC data within a multi-tenanted environment could result in unauthorized access to and use or disclosure of OPC data. This would put OPC in breach of principle 5 and cause harm to OPC customers or employees or to OPC's reputation.	Azure uses virtual networking to isolate tenants' traffic from one another, employing measures such as host- and guest-level firewalls, IP packet filtering, port blocking, and HTTPS endpoints. Most of Azure's internal communications, including infrastructure-to-infrastructure and infrastructure-to-customer (on-premises), are encrypted.	Minor	For communications within an Azure datacentre, Microsoft manages networks to ensure that no VM can impersonate or eavesdrop on the IP address of another. SSL/TLS is used when accessing Azure storage or SQL databases, or when connecting to cloud services.	Minimal

Principles 6 and 7: Access to and correction of information

Ref. no.	Responding to requests for information or requests to correct information	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-6.1	OPC must respond to subject access and correction requests in compliance with principles 6 and 7 and, in particular, within Privacy Act timeframes.	The use of the Microsoft Azure solution might impact on OPC's ability to meet its obligations under principles 6 and 7 due to an inability to access the information for reasons outside OPC's control.	A failure to meet the timeframes required by the Privacy Act or to properly manage a subject request could put OPC in breach of principles 6 or 7, cause harm to a data subject and damage OPC's reputation.	In its OST, Microsoft promises that at all times during subscription, the customer will have the ability to access, extract and delete data stored in each online service. Further, in its OST, Microsoft states that it will assist a customer to meet its obligations to data subjects, including access (and notes that it will redirect any requests from a data subject to the customer).	Minimal	N/A	Minimal

Principle 8: Accuracy etc. of personal information to be checked before use

Ref. no.	Steps taken to check accuracy, relevance etc. before use?	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-8.1	OPC must take reasonable steps to ensure that personal information is accurate etc before using or disclosing it.	Move to Azure does not impact on compliance with principle 8.	N/A	N/A	N/A	N/A	N/A

Principle 9: Agency not to keep personal information for longer than necessary

Ref. no.	How long do you keep personal information and why?	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-9.1	OPC must retain personal information only as long as necessary, in accordance with Public Records and Official Information Acts.	Microsoft or one of its subprocessors retains OPC personal information for longer than OPC's lawful purposes require.	OPC is in breach of its legal obligations. An associated risk of disclosure or unauthorised use if information is replicated or backed-up.	During the term of its subscription with Microsoft, OPC has full control over the retention of its data and can delete it directly. In its OST, Microsoft promises to retain customer data for 90 days after the termination of a subscription so that the customer may extract it. After 90 days, the data is deleted (unless there is a legal requirement to retain it).	Minimal	N/A	Minimal

Principle 10: Use of information

Ref. no.	What are you going to use the personal information for?	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-10.1	OPC must ensure that the personal information it holds is used only for the purposes for which it was collected (that is, its statutory functions and activities).	Microsoft or its subprocessors could use personal information about OPC customers or employees for other purposes not related to the purposes for which OPC collected it (such as for marketing purposes).	An unauthorised use of personal information by Microsoft or its subprocessors could put OPC in breach of principles 5 or 10 and could cause harm to individuals and to OPC's reputation.	In its OST, Microsoft states that customer data will be used only to provide the customer with online services, and that data will not be used for any other purpose, including advertising. In its OST, Microsoft also states that it is responsible for ensuring that its subprocessors will not use customer data for any purpose other than delivering the specific services Microsoft has requested. Further, if Microsoft uses data for other purposes, it will be in breach of the Australian Privacy Act.	Minimal	Request audit reports to substantiate assurances and contractual provisions.	Minimal

Principle 11: Disclosure of information

Ref. no.	Who are you going to disclose the personal information to (if anyone) and why?	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-11.1	Disclosure of OPC data to Australian government or law enforcement agencies.	Microsoft may be required by law to disclose OPC data to third parties, including law enforcement agencies.	While it may not breach the Privacy Act (by virtue of section 10), the disclosure of OPC data by a cloud provider could undermine OPC's ability to be directly accountable for the protection of the personal information it holds and undermine public trust in OPC.	In its OST, Microsoft states that it will not release information to any third party voluntarily and will seek to redirect all such requests to OPC. Where required to comply with a legal order to disclose, Microsoft will promptly advise OPC. Microsoft undertakes not to give any third party unfettered access, encryption keys, or access in the knowledge that the information will be used for purposes wider than the lawful request. Microsoft has evidenced its approach to challenging lawful requests (see the Irish case).	Minor	OPC has also discussed this issue directly with Microsoft legal staff, who have provided further assurances about the likelihood of lawful requests for enterprise data, noting that most lawful requests are for data about individual account holders. OPC should monitor any changes to the OST to ensure that the current assurances remain unchanged.	Minimal

Ref. no.	Who are you going to disclose the personal information to (if anyone) and why?	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-11.2	Disclosure of OPC data to overseas government or law enforcement agencies (including United States agencies)	Microsoft may be required to disclose OPC data to overseas agencies, either where data has been transferred to a third country or where the data remains in Australia but an overseas agency makes a request of Microsoft under international law or a national law deemed to have extra-territorial effect.	While it may not breach the Privacy Act (by virtue of section 10), the disclosure of OPC data by a cloud provider could undermine OPC's ability to be directly accountable for the protection of the personal information it holds and undermine public trust in OPC. Microsoft makes it clear that it may store data in other countries in some circumstances (such as periods of civil unrest in the selected geographic region). Further, it states that some services require data to be stored, even temporarily, outside a specific geographic region. In any event, Microsoft Corporation may receive requests from third country agencies regardless of the data centre location, e.g. under US CLOUD Act.	OPC will select that its data is stored in the Australian geographic region. This will reduce the likelihood, at least, of data at rest being subject to other jurisdictions. The provisions in the OST regarding third party requests, as noted above, also apply to requests from agencies in third countries.	Minimal	OPC should actively monitor this issue and ensure that it is made aware of any decisions by Microsoft to move data at rest outside the specific geographic region. However, in all cases the likelihood of third country agencies making lawful requests for OPC data is low.	Minimal

Principle 12: Use of Unique Identifiers

Ref. no.	Why do you need a unique identifier, and are you allowed to use this one?	Description of the risk identified	Rationale and consequences for the agency or individual	Existing controls that contribute to manage risks identified	Assessment of residual (current) risk recognising current measures	Recommended additional actions to reduce or mitigate risk	Residual risk remaining despite new safeguards
R-12.1	OPC does not assign unique identifiers	The move to Azure does not impact on compliance with principle 12.	N/A	N/A	N/A	N/A	N/A