Complying with Australian privacy requirements when using Microsoft's cloud services

Updated: 23 Nov. 17.

This document provides information about Microsoft's commitments to assist and facilitate customers to meet their privacy obligations when using Microsoft's public cloud services, in particular under the Australian Privacy Principles and *Privacy Act 1988* (Cth) (**Privacy Act**). This information is arranged as follows:

1. Information about the Microsoft public cloud services
2. Microsoft's approach to privacy compliance
3. Microsoft's position on the *Privacy Act* requirements
4. Other frequently asked questions from customers about privacy compliance

Microsoft does not provide its customers with legal advice and nothing in this document should be construed as such. Customers should obtain their own independent legal advice. Microsoft provides the online services on the basis that each customer has complied with its own privacy obligations.

Microsoft's approach to privacy compliance

When moving to a public cloud solution, Microsoft's approach is to work collaboratively with customers to translate their existing compliance practices to reflect the new environment and empower them to control the collection, use, handling, integrity and distribution of their data.

This approach does not mean that Microsoft can or will directly assume its customers' many and varied compliance obligations. Microsoft's public cloud services are offered to all customers on the same basis and with the same functionality. Assuming such a burden would limit Microsoft's cloud service functionality for all its customers to address the compliance risks faced by a select few. Instead, Microsoft believes that cloud providers and cloud service users need to work together to address privacy concerns in a thoughtful and scalable manner. This is Microsoft's collaborative approach to privacy compliance.

Microsoft and the Privacy Act

Microsoft's collaborative approach to privacy compliance applies equally to Australian privacy legislation.

Australian privacy legislation applies to many organisations in relation to their dealings with personal information, being information or an opinion about an individual who is identified or reasonably identifiable. The legislation with the broadest reach is the *Privacy Act 1988* (Cth), which sets out in schedule 1 a set of thirteen Australian Privacy Principles (**APPs**) imposing requirements for collecting, holding, using and disclosing personal information on affected organisations. Broadly speaking, the requirements imposed by the APPs are similar to the requirements that are imposed by other Privacy Principles under Australian law (including under State and Territory legislation).

When considering Microsoft online services, customers should be aware of the following in-built features and attributes which are common to all Microsoft online services:

1. Microsoft uses customer data only for the purposes of providing the services
2. Microsoft does not collect or use any personal information contained in the customer's data
3. Data centres holding customer data are independently verified to meet strict security requirements[1]
4. Customers retain all rights in, and effective control of, their data; customers can extract, verify, amend or delete their data at any time
5. Microsoft will not provide any third party direct, indirect, blanket or unfettered access to customer's data except as directed by a customer or required by law
6. After customers terminate the service, all of their data is deleted.[2]

[1] For a full description of our security architecture and information security practices please refer to our response to the Cloud Security Alliance's Cloud Control Matrix at: http://www.microsoft.com/download/en/details.aspx?id=26647.

Customers should incorporate a review of Microsoft's data privacy commitments, which include the general principles set out above, as part of the general review of the Microsoft online services. At the end of this review process, customers will be able to determine whether or not the Microsoft online services enable, or can be configured to enable, the customer to remain compliant with its regulatory (including privacy) obligations.

To assist with this process, Microsoft has created a detailed table (set out on pages 4 and 5 of this paper) which outlines each APP requirement, and then sets out Microsoft's position on each requirement. The Microsoft position in each case is generated based on the general principles described in this paper.

Mandatory Data Breach Notification

Microsoft makes a commitment in the "Security Incident Notification" section of the Online Services Terms3 to:

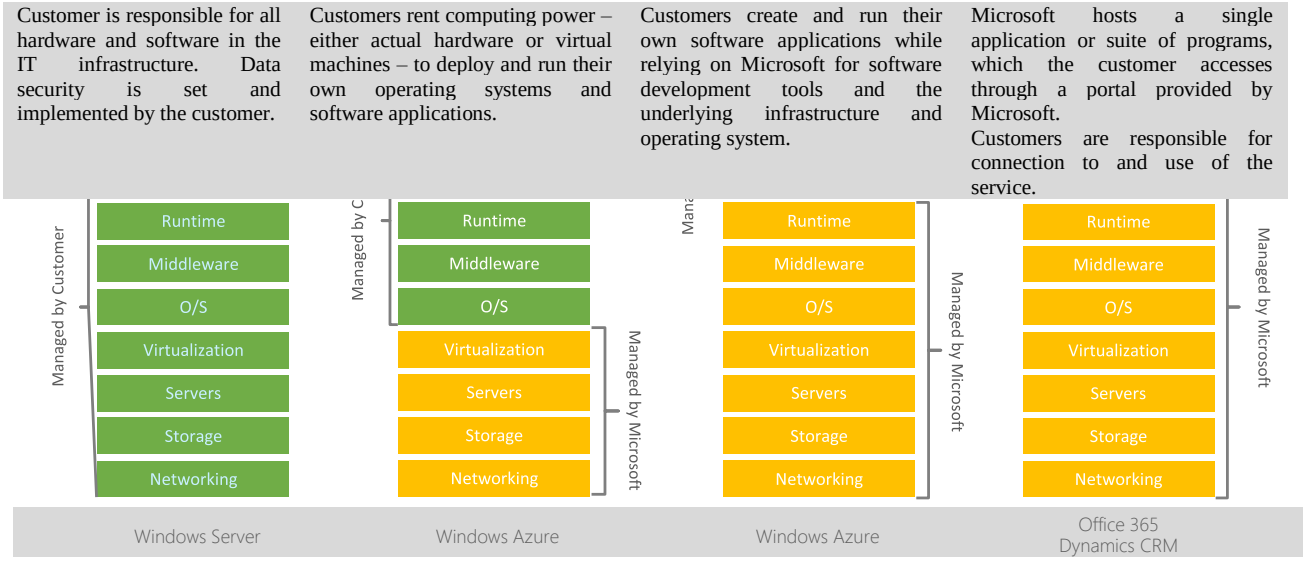
1. notify customers of any security incident (as defined in the Online Services Terms);
2. investigate the security incident
3. provide Customer with detailed information about the security incident; and
4. take reasonable steps to mitigate the effects and to minimize any damage resulting from the security incident.

Microsoft does not look at the data customers put into our Online Services. So Microsoft has no way to know (a) whether Customer Data includes personal information; or (b) who such information might relate to.

It is therefore the customer's responsibility to undertake a "reasonable and expeditious assessment" as to whether there are reasonable grounds to believe an eligible data breach has occurred, and then, if necessary, to notify the affected individuals and the Office of the Australian Information Commissioner.

Microsoft public cloud services

Microsoft offers a range of public cloud services and infrastructures to purchase. Identifying the most appropriate cloud model depends on customer needs, data control requirements and type of processing required. Below is a chart comparing our public cloud services to a customer's existing on premises IT infrastructure.



This document focuses on Microsoft's public cloud service offerings. For customers with more specialised data protection requirements, Microsoft has private and hybrid cloud solutions which may be more appropriate. For a more detailed comparison of public, private and hybrid cloud solutions, please refer to www.whymicrosoft.com.

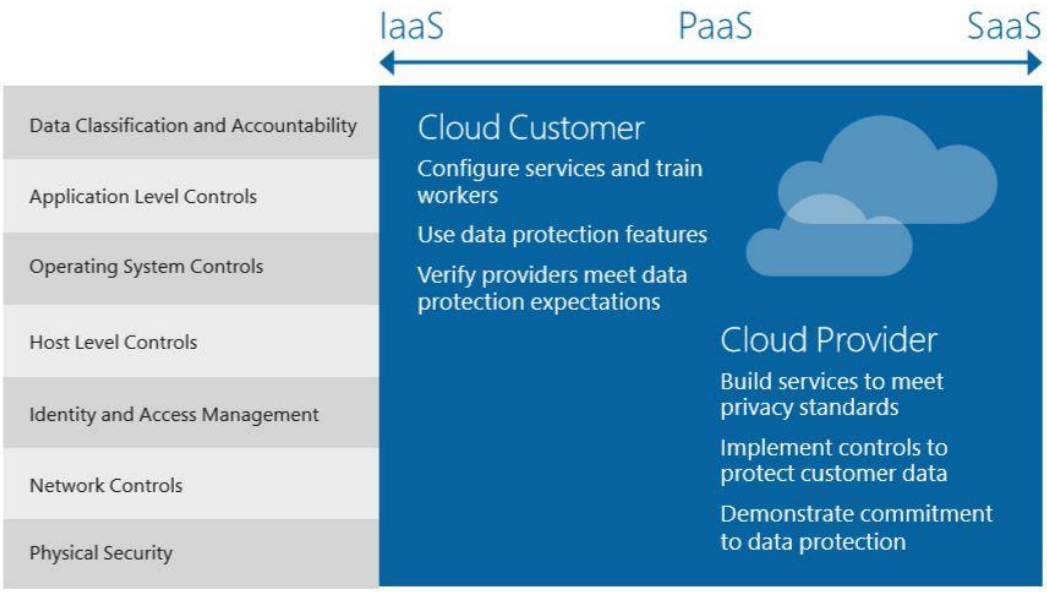
---

[2] Customer Data is held for at least 90 days for data to be extracted or migrated to a new service, and after this period it is deleted within a further 90 days.

[3] Available at https://www.microsoft.com/en-us/Licensing/product-licensing/products.aspx.

Collaborative Approach

The collaborative approach requires an allocation of roles and responsibilities and at Microsoft, we work to be as transparent as possible about this. Unfortunately, the boundaries are not always clear cut, and can depend on the service and other factors. Below is a chart that reflects the allocation of responsibility as between Microsoft as cloud service provider, and cloud service customers.



Microsoft holds itself responsible for the platform and accountable for creating a service that can be configured to meet the security, privacy and compliance needs of its customers. Microsoft has industry-leading, independently verified data security processes and requirements in-built to its services and the shared experience of supplying hundreds of cloud and online solutions to hundreds of millions of customers worldwide. We believe that our time-tested processes and procedures embedded in the operation of our public cloud solutions provide a solid foundation to address our customers' concerns.

In turn, customers are responsible for configuring and operating their public cloud solution after it has been provisioned, including managing access credentials and regulatory and legal compliance, protecting applications through the service's configurable controls, data content and any virtual machines or other data that they use with their account. Microsoft provides the tools and platform to enable its customers to meet their obligations, but it is up to the customer to learn and configure those tools.

In addition to designing and implementing customer-configured controls, Microsoft demonstrates its commitment to data protection by obtaining certifications, sharing attestation reports and signing agreements. Microsoft makes these materials available to allow customers to verify and decide for themselves whether Microsoft's public cloud services meet their organisational data protection expectations.

APP Summary Table

APP	Summary of obligations	Microsoft's position
Open and Transparent Management principles 1.2 1.3-1.6	An entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities to ensure compliance with the APPs or an APP code; and enable the entity to deal with inquiries or complaints about compliance with the APPs or an APP code	Microsoft's handling, use and control over customer data is limited; so the APPs apply in a similarly limited fashion. Microsoft believes the architecture of the online services, supported by contractual commitments, are reasonable steps to ensure that the service complies with the APPs. This is reflected in the certifications that Microsoft obtains and maintains for all Microsoft Online Services. Customers retain all rights in their customer data and retain effective control over all data they elect to collect, upload into the online services and use or disclose as part of their business. Accordingly, the bulk of the obligations imposed by the APPs remain with the customer. Microsoft provides many configurable built-in features (including encryption of data in transit and at rest) to support customers' compliance.
	An entity must have a clearly expressed and up to date privacy policy containing information about how the entity collects, holds, uses and discloses personal information. An entity must make this privacy policy available free of charge and in an appropriate form.	Each customer remains responsible for maintaining and making available a privacy policy of its own that complies with the APPs. Microsoft supports customer compliance by, for example, committing not to use customer data except for providing the service, facilitating data encryption in the service, and implementing data deletion policies.
Anonymity and identifier principles 2, 9	Entities must, where lawful and practical, give individuals the option of not identifying themselves. Entities must not adopt a government-related identifier nor use or disclose a Commonwealth identifier unless certain limited exceptions apply.	Each customer remains responsible for ensuring its use of personal information does not adopt, use or disclose unique identifiers, except within the limited parameters prescribed by the APPs. Microsoft supports customer compliance by, for example, committing not to use customer data except for providing the service, facilitating data encryption in the service, and implementing data deletion policies.
Collection Principles 3-5	Outline of when an entity can collect personal information. Entities that collect personal information must make an individual aware of certain prescribed matters.	Each customer remains responsible for collecting personal information (including sensitive information) in a manner compliant with the APPs, including providing notification to the individual of prescribed matters. Microsoft supports customer compliance by, for example, allowing classification of customer data, providing the means to restrict access to customer data and committing not to use customer data except for providing the service.
Use and disclosure principles 6-7	Outline the parameters within which an entity may use or disclose personal information that it holds. Sets out conditions which must be met before personal information may be used or disclosed for any purpose secondary to the purpose for which it was collected, including for sales or direct marketing purposes.	Microsoft will not use or disclose customer data to any third party without the customer's instruction or a lawful government access request. In addition, Microsoft will only use personal information for the purposes of providing the online services and will not mine data for advertising or any other secondary purpose. This is a key feature of the ISO 27018 code of practice against which Microsoft is audited annually. When it comes to the use of each online service, each customer remains responsible for ensuring its use and disclosure of personal information stored within or used via the service is consistent with the APPs. Microsoft supports customer compliance by, for example, facilitating record-keeping of all media on which customer data is stored and committing not to use of customer data except to provide the service.

APP	Summary of obligations	Microsoft's position
Cross-border disclosure of personal information 8	Entity must take reasonable steps to ensure an overseas recipient (who is not the entity) does not breach the APPs before disclosing personal information to that overseas recipient.	The Australian Government's Better Practice Guide, *Privacy and Cloud Computing for Australian Government Agencies*, states that: *"If an agency shares personal information with a contracted cloud service provider, this may be considered a "use" rather than a "disclosure" under the Privacy Act, depending on the degree of control the agency retains over the personal information. An agency that gives up its control over personal information to an outsider is treated as disclosing that information. An agency that maintains control over personal information is treated as using that information"*. Based on this guidance, there will be no disclosure of personal information when utilising Microsoft cloud services as Microsoft only processes personal information provided by its cloud customers in accordance with its customer's instructions. Microsoft is bound by the obligations and commitments set out in its customer contracts (including the Online Services Terms) and is held to the same standards for which the Online Services are certified (such as ISO 27001 and ISO 27018) irrespective of where a customer's data is processed. Microsoft also discloses on a published websites and provides tools in the Online Service so customers can find out where their customer data is sent in the world. Customers may use this information in obtaining the necessary consents from individuals for transfers of personal or sensitive information.
Storage, access and accuracy principles 10-12	Obligations and steps around protecting the integrity of personal information, including the quality, duration of retention, security, access to and correction of personal information	Microsoft protects the integrity of customer data by maintaining multiple redundant copies of data to minimise risk of loss or corruption. Customer data is held in data centres which are independently certified to ISO 27001 standards and verified by annual compliance audits (audit reports can be made available to customers on request). Microsoft contractually commits to not disclose customer data to any third party (including the individual) except upon instruction or permission by the customer, or if required by a lawful demand. Microsoft also regards customer data as confidential. We believe that these steps constitute reasonable steps to assure the security and integrity of customer data. Customers retain effective control of their data and can take reasonable steps to ensure the accuracy and integrity of the personal information collected, and the duration for which it is held, as well as to provide access to, or correct, personal information upon request or on its own initiative.

Other frequently asked questions

Where is the personal data of Microsoft customers or customer's end users being stored?

Microsoft believes that it is important to be transparent on these issues and provides this information on the individual Trust Centres for each service (links to which are on page 7 of this paper) and as set out in the Online Services Terms.

What assurances will Microsoft give that Customer data will be stored securely?

No other cloud provider offers the breadth of trust features we do across cloud platforms. For example, we meet or exceed ISO 27001, a security certification that sets out a series of physical, process and management controls and we are the only hyper-scale cloud service provider certified for compliance with the ISO 27018 code of practice – the first international privacy standard for cloud services. Microsoft is also the first cloud provider to receive the endorsement of European Union's 28 data protection authorities (acting through their "Article 29 working party") that its contractual privacy protections meet current EU standards for international transfers of data.

For a full description of our security architecture and information security practices please refer to our response to the Cloud Security Alliance's Cloud Control Matrix at: http://www.microsoft.com/download/en/details.aspx?id=26647

What happens if there is a privacy breach?

Microsoft contractually commits to notifying customers promptly in the event of a breach affecting their data, and in any event within at least 5 calendar days. In addition, this process is validated on an annual basis to ISO 27001 and ISO 27018 standards through the independent certification and annual audit processes applicable to the Microsoft online services.

What is Microsoft's position on the EU General Data Protection Regulation?

Microsoft's cloud business is grounded in four commitments. The security of data is our priority. We will ensure people's data is private and under their control. We will figure out the laws in each country and make sure data is managed accordingly. And we will be transparent so people know what we are doing.

The EU General Data Protection Regulation (GDPR) is a welcome step forward for the EU and is aligned with our cloud commitments. We will ensure that Microsoft complies with GDPR as it applies to Microsoft when it goes into effect in May 2018. We'll share more specific details as our plans are finalized and will stand behind our contractual commitment to "comply with all laws and regulations applicable to our provision of the Online Services."

Who has access to customer data?

Microsoft employees and contractors only have access to customer data for the purpose of maintaining and providing the online services. This includes troubleshooting assistance and malware prevention purposes. Prior to receiving access to non-public customer data, all subcontractors are required to successfully complete a background check and enter into written agreements entrenching at least those commitments Microsoft offers as standard, All such subcontractors are listed on the Trust Centre for each applicable online service. In addition, ISO 27018 certification verifies that Microsoft has executed binding contracts with each subcontractor that include the same security and personal data protection obligations that Microsoft commits to.

Subject to those limited rights to use or access customer data granted to Microsoft and its staff, all right, title and interest in and to customer data remain with customers. Customers may grant access to any other party at will, and Microsoft online services provide access privileges and identity management software that can be used to control that access to customer data.

How does Microsoft respond to requests by government agencies to access customer data?

Microsoft has been vocal in its position that governments should only be able to access data in accordance with a process that is transparent and in accordance with the rule of law. Microsoft first lobbied, then ultimately sued the U.S. government to be able to disclose more information about the requests it receives.

Microsoft's General Counsel, Brad Smith, has posted a number of articles on the Microsoft on the Issues blog (http://blogs.technet.com/b/microsoft_on_the_issues) which are intended to provide the public with information on Microsoft's approach in this area. Customers concerned about this issue should read these articles as they contain a large amount of useful information.

As an example, the following four points are extracted from one such article:[4]

- Microsoft does not provide any government with direct and unfettered access to our customer's data. Microsoft only pulls and then provides the specific data mandated by the relevant legal demand.
- If a government wants customer data – including for national security purposes – it needs to follow applicable legal process, meaning it must serve us with a court order for content or subpoena for account information.
- We only respond to requests for specific accounts and identifiers. There is no blanket or indiscriminate access to Microsoft's customer data. The aggregate data we have been able to publish shows clearly that only a tiny fraction – fractions of a percent – of our customers have ever been subject to a government demand related to criminal law or national security.
- All of these requests are explicitly reviewed by Microsoft's compliance team, who ensure the requests are valid, reject those that are not, and make sure we only provide the data specified in the order. While we are obligated to comply, we continue to manage the compliance process by keeping track of the orders received, ensuring they are valid, and disclosing only the data covered by the order.

In addition, Microsoft is committed to notifying business and government customers if we receive legal orders related to their data. Where we are prohibited from doing notifying our customers, we will challenge this prohibition in court. Microsoft will also assert available jurisdictional objections to legal demands when governments seek this type of customer content that is stored in another country.

Microsoft also publishes a Law Enforcement Requests Report (www.microsoft.com/transparency) on a 6 monthly basis. This Report contains detailed statistics as to the disclosure requests that Microsoft has received during the reporting period. As of the date of this document, Microsoft has not been compelled to provide customer data for any enterprise customer based outside the U.S. for any reason.

Where is Microsoft's Privacy Statement?

For government and business customers acquiring public cloud services under a volume licensing agreement, our privacy commitments are set out in the Online Services Terms. The current version of the Online Services Terms is accessible at www.microsoft.com/contracts.

Outside the volume licensing context, you can find our general privacy statement and links to privacy statements for the majority of our products and services here: http://www.microsoft.com/privacystatement/en-au/core/default.aspx

Where can Microsoft's Trust Centres be found?

Microsoft trust centres for its public cloud services can be accessed at the following hyperlinks:

- Office 365: http://www.trustoffice365.com
- Microsoft Azure: http://azure.microsoft.com/en-us/support/trust-center/
- Dynamics CRM: http://www.microsoft.com/en-us/dynamics/crm-trust-center.aspx
- Windows Intune: http://www.microsoft.com/en-us/WindowsIntuneTrust/

[4] See: http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/07/16/responding-to-government-legal-demands-for-customer-data.aspx