



Privacy in Microsoft Cloud Services

Published: June 26, 2017

This document provides details on Microsoft's privacy principles and privacy standards, which guide the collection and use of customer and partner information and give our employees a clear framework to help ensure that we manage data responsibly

Introduction	2
Microsoft Commitment to Customer Privacy.....	2
Microsoft Corporate Privacy Policy and Microsoft Privacy Standard	3
Microsoft's Policy Activities for Privacy	3
Microsoft's Approach to Regulatory Compliance.....	4
Support for EU-U.S. Privacy Shield	4
General Data Protection Regulation	5
Microsoft Trust Center	5
Service Trust Preview and Office 365 Service Assurance	6
Privacy in Microsoft Cloud Services	6
Global Privacy Information	8
Argentina	9
Australia.....	10
Brazil.....	14
Canada	14
Finland	18
Malaysia.....	19
Mexico	20
Morocco.....	24
Nigeria.....	25
New Zealand.....	26
Poland.....	27
Singapore	32
South Africa.....	34
Taiwan.....	37
Thailand.....	38
Microsoft Privacy Resources	40
Summary	40

Introduction

At Microsoft, we believe privacy starts with putting our customers in control and providing the tools and information that customers need to make informed choices. Microsoft has been considering and addressing privacy issues associated with cloud computing and online services since the launch of The Microsoft Network (MSN) in 1994, and we remain committed to protecting our customer's privacy.

Microsoft works to responsibly manage and protect data we store, to be transparent about our privacy practices, and to offer meaningful privacy choices. These three tenets—responsibility, transparency, and choice—are the foundation of Microsoft's approach to privacy.

Privacy is also a pillar in all our business models. We understand that strong privacy protections are essential for building trust in cloud services and for helping cloud computing reach its full potential. That's why we build and operate our cloud services with privacy and strong data protection in mind.

Microsoft understands that when you, our customer, use our business cloud services, you are entrusting us with your most valuable asset—your data. You trust that its privacy will be protected and that it will be used only in a way that is consistent with your expectations. Our time-tested approach to privacy is grounded in our commitment to give you control over the collection, use, and distribution of your [customer data](#). We are transparent about our policies, our operational practices, and the controls and technologies we use to help ensure the privacy of your data in Microsoft business cloud services.

Microsoft Commitment to Customer Privacy

As part of our long-term commitment to [Trustworthy Computing](#), Microsoft strives to earn and strengthen trust by building robust privacy and data protections into our products and services. A dedicated team at Microsoft focuses on guiding development teams to deliver secure, privacy-focused, and reliable computing experiences based on sound business practices. The privacy group manages our privacy governance program, which includes ongoing employee training, identification of emerging privacy issues in the industry, and regular updates to our privacy standards.

To put our principles and standards into practice, we have invested heavily to build a comprehensive privacy governance program. Microsoft employs many full-time privacy professionals, with several hundred other employees helping to ensure that privacy policies, procedures, and technologies are applied across our products and services. In addition, Microsoft's global privacy community helps to ensure that our privacy policies, procedures, and technologies are applied within our business units. The privacy community includes a three-tiered group of privacy champions, leads, and managers who work with developers, marketers, lawyers, and business executives to review Microsoft products and services, and to provide guidance on privacy-related issues.

Microsoft Corporate Privacy Policy and Microsoft Privacy Standard

The Microsoft Corporate Privacy Policy comprises six key principles for the protection and appropriate use of customer information, such as information submitted by customers, data obtained from third parties, and data that is collected automatically.

Microsoft's six key privacy principles are:

Control

We will put you in control of your privacy with easy-to-use tools and clear choices.

Transparency

We will be transparent about data collection and use so you can make informed decisions.

Security

We will protect the data you entrust to us through strong technical and organizational security measures and state-of-the-art encryption mechanisms.

Strong legal protections

We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right.

No content-based targeting

We will not use your email, chat, files, or other personal content to target ads to you.

Benefits to you

When we do collect data, we will use it to benefit you and to make your experiences better.

These principles form the foundation of Microsoft's approach to privacy and they will continue to shape the way we build our products and services. Microsoft's consumer and business products and services are developed with strict adherence to [Microsoft's privacy standards and principles](#). These standards inform Microsoft employees and vendors about how to develop products and services with customer privacy in mind so that customers can better understand and control the collection, storage, retention, destruction, and use of their data.

Microsoft's Policy Activities for Privacy

Microsoft works with governments, businesses, technology leaders, and civil society to advise on legislative proposals, help align laws across jurisdictions, develop responsible privacy practices, and strengthen self-regulatory mechanisms that support privacy and data protection in the data age. For example, we have long supported baseline US privacy legislation, coupled with industry self-regulation that facilitates the free flow of information, enhances privacy and trust, and encourages innovation.

Microsoft has joined with several other companies in an initiative to limit governments' authority to collect users' information, to enact oversight for intelligence agencies that are collecting or compelling the production of information. For more information, visit the [Reform Government Surveillance](#) site. Microsoft has also created a [Digital Constitution](#) web site that provides information about topics such as Microsoft's legal challenge to a U.S. Government search warrant, and balancing rights in a global cloud.

Finally, Microsoft supports the concept of accountability. Under an accountability model, privacy goals are established in law, but individual organizations are responsible for determining how best to meet those goals. Further, we have supported efforts to create greater interoperability among global privacy frameworks that allow differing data protection regimes to work together to support compliance, privacy, and innovation. Together with privacy stakeholders from around the world, we are also thinking about how to evolve the frameworks that have governed aspects of the protection of personal data for the data age.

Microsoft's Approach to Regulatory Compliance

To help organizations comply with national, regional, and industry-specific requirements governing the collection and use of individuals' data, Microsoft offers the most comprehensive set of certifications and attestations of any cloud service provider. To demonstrate that these controls deliver compliance you can rely on, Microsoft enterprise cloud services are independently validated through certifications and attestations, as well as third-party audits. In-scope services within the Microsoft Cloud meet key international and industry-specific compliance standards, as well as regional and country-specific standards and contractual commitments. In addition, rigorous third-party audits validate the adherence of our cloud services to the strict requirements these standards mandate.¹

Just as Microsoft has a responsibility to process our customers' information in a trustworthy manner, many of our enterprise customers have a responsibility to comply with national, regional, and industry-specific requirements. As a global provider of cloud services, we must run our services with common operational practices and features that span multiple customers and jurisdictions. To fulfill our privacy responsibility to our customers, as well as help our diverse customer base fulfill its regulatory obligations, we set the bar high and then build our services to meet that bar using common privacy and security controls. While it is ultimately up to our customers to assess whether our services satisfy their specific regulatory needs, we are committed to providing detailed information about our cloud services to help customers with their assessments.

Support for EU-U.S. Privacy Shield

Microsoft supports the [EU-U.S. Privacy Shield](#), which sets a high standard for the protection of Europeans' personal data. The Privacy Shield secures Europeans' right to legal redress, strengthens the role of data protection authorities, introduces an independent oversight body, and it clarifies data collection practices by U.S. security agencies. In addition, it introduces new rules for data retention and onward transfer of data.

On August 1, 2016, Microsoft signed up for the EU-U.S. Privacy Shield and submitted its Privacy Shield certification to the U.S. Department of Commerce. Microsoft was the first global cloud provider to be

¹ Customers can view by service, location, and industry, all the global standards to which Microsoft cloud services conform on the [Compliance](#) page of the Microsoft Trust Center.

approved for Privacy Shield on August 12, 2016. Going forward, any data which we will transfer from Europe to the United States will be protected by the Privacy Shield's safeguards.²

General Data Protection Regulation

In May 2018, a European data privacy law is due to take effect that will require big changes, and potentially significant investments, by organizations all over the world—including Microsoft and our customers. Known as the [General Data Protection Regulation](#) (GDPR), the law imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents. The GDPR applies no matter where you are located.

Microsoft believes the GDPR represents an important step forward for individual privacy rights. It gives EU residents more control over their "personal data" (which is precisely defined by the GDPR). The GDPR also seeks to ensure that personal data is protected no matter where it is sent, processed, or stored.

The GDPR contains many requirements about how personal information is collected, stored and used. This means not only how you identify and secure the personal data in your systems, but also how you accommodate new transparency requirements, how you detect and report personal data breaches, and how you train privacy personnel and employees.

We recommend you begin your journey to compliance with the GDPR by visiting our [GDPR](#) web site and reviewing our GDPR whitepapers:

- [An Overview of the General Data Protection Regulation \(GDPR\)](#)
- [Beginning your General Data Protection Regulation \(GDPR\) Journey](#)

Microsoft Trust Center

Although many organizations cite privacy and security concerns as major obstacles to their adoption of cloud services, information on the privacy and security practices of many cloud providers is either difficult to find or indecipherable to all but the most astute IT professionals. To help our customers find answers to their privacy and security questions about our cloud services, we strive to be as transparent as possible about our data protection policies and procedures.

The centerpiece of our transparency efforts is the [Microsoft Trust Center](#), an online repository of detailed information about the privacy and security practices in Microsoft Azure, Microsoft Office 365, Microsoft Dynamics, Microsoft Intune, Microsoft Power BI, and other cloud services. The Microsoft Trust Center also includes several service-specific Trust Centers:

- [Office 365](#)
- [Microsoft Azure](#)
- [Microsoft Commercial Support](#)

² See <http://blogs.microsoft.com/on-the-issues/2016/08/01/microsoft-signs-privacy-shield/> for the official announcement.

- [Microsoft Dynamics AX](#)
- [Microsoft Dynamics 365](#)
- [Microsoft Intune](#)
- [Microsoft National Clouds](#)
- [Power BI](#)

The Microsoft Trust Center is designed to provide answers to questions that customers have about our cloud services, such as who can access their data, where their data is stored, and how they can verify that Microsoft is doing what it says. Our compliance is independently audited, and we're transparent on many levels—from how we comply with regulatory requirements, to how we handle legal demands for customer data, to the security of our code. For example, on the [Regulatory Compliance](#) page, we explain how we believe our services help facilitate compliance with a range of major statutes, from European Union data protection laws to the U.S. Gramm-Leach-Bliley Act, which includes provisions on the protection of consumers' financial information.

We also provide customers with detailed information about the well-recognized certifications that our cloud services have attained. On the [Security, Audits, and Certifications](#) page, customers can locate information about the certifications held by our cloud services and the Microsoft datacenters that host those services.

Service Trust Preview and Office 365 Service Assurance

Many of our customers in regulated industries are subject to extensive compliance requirements. To perform their own risk assessments, customers often need in-depth information on how our Microsoft maintains the security and privacy of customer data within our cloud services. Microsoft is committed to the security and privacy of customer data in its cloud services and to earning customer trust by providing a transparent view of its operations, and easy access to independent compliance reports and assessments.

On the [Service Trust Preview](#) site and within the Office 365 [Service Assurance](#) dashboard, we enable customers to download third-party audit reports for all our enterprise online services. By making this information readily available, we empower customers to validate that what we say about our security and privacy practices has been affirmed by an accredited third party. Service Assurance also provides customers with information about how Microsoft's cloud services maintain security, privacy and compliance with global standards. The Service Assurance area includes independent third-party audit reports for our cloud services, and implementation and testing details for the security, privacy, and compliance controls used by Microsoft to protect customer data.

Privacy in Microsoft Cloud Services

Microsoft recognizes that cloud services often raise unique security and privacy questions for business, education, and government customers, so we have adapted our policies and governance programs to address customer concerns, facilitate regulatory compliance, and to build greater trust in

cloud computing and our cloud services. For example, we contractually commit to specific data handling processes as part of our agreements for our cloud services. We also provide customers with flexible management tools that help protect sensitive data and support compliance with government privacy and security guidelines. For example, tenant administrators can control how an organization's data is shared externally, between users, and how it is used within the cloud service, as well as configure other [advanced privacy options](#). Such transparent policies and strong tools are essential for our customers as they deal with the privacy and security questions that arise from their use of cloud services.

All Microsoft cloud services undergo privacy reviews that are designed to identify privacy requirements and help product teams follow Microsoft privacy policies and standards and various national and international industry certification standards (e.g., ISO 27001/27018, SOC/SSAE 16, FedRAMP, etc.). Microsoft uses a variety of risk management mechanisms to appropriately manage regulatory change, organizational change, personnel change, and technological change. Before any cloud service launches to the public, subject-matter experts conduct privacy, security, and business continuity risk assessments on each service and work closely with the service owners to remediate any identified risks. After launch, we use a process of continuous monitoring to ensure that our data protection systems are functioning properly. We test required functionality annually, semi-annually, quarterly, monthly, or at the time of each new release, depending on the level of risk associated with the privacy or security control. We also conduct regular risk assessments to refresh the control framework and, if necessary, to reset priorities if new aspects of the service emerge as high-risk. This multi-layered and continuous approach to monitoring the data protection environment helps us quickly diagnose and remedy problems that occur and helps our customers respond quickly to shifting regulatory or industry requirements.

Microsoft understands that strong privacy protections are essential for building trust in cloud computing, and implements them as follows:

- **Data use** Microsoft details how [we manage and use customer data](#), and provides explicit statements that Microsoft uses customer data only for providing cloud services. Microsoft does not build advertising products out of our customers' data. We also don't scan our customers' email or documents for building analytics, data mining, advertising, or improving our services without our customers' permission.
- **Shared data storage** To enable cost savings and efficiencies for data storage, Microsoft stores customer data from multiple customers on the same equipment (known as a *multi-tenant* architecture). However, we go to great lengths to help ensure that multi-tenant deployments of cloud services such as [Office 365](#), [Azure](#), [Dynamics 365](#), and others logically separate the data (and the processing thereof) of different accounts and support the privacy and security of the data stored.
- **Data portability** During the term of a subscription to Microsoft business services, customers can access and extract their customer data. Customers of Azure, Dynamics 365, Intune, and Office 365 in-scope services can retrieve a copy of their customer data at any time and for

any reason, without the need to notify Microsoft or ask for assistance. Also, you can [take your customer data with you](#) if you end your subscription.

- **Transparency** The [Microsoft Trust Center](#) details the policies and practices that Microsoft uses to protect customer data. The [Microsoft Transparency Hub](#) provides customers with direct access to several reports regarding law enforcement and government requests for customer data.
- **Access** Microsoft personnel and any subcontractors it employs do not have standing access to customer data. Microsoft identifies [who can access customer data](#) and the circumstances under which they can access it. Microsoft also logs and reports all access to customer data and other critical data. Additionally, Microsoft and its third-party auditors conduct sample audits to verify that the customer's data is accessed only for appropriate business purposes.
- **Geographic location of data** Microsoft provides details about where online services are located and where customer data is stored. We contractually commit to storing customer data in predetermined geographic areas. Administrators can choose to receive updates to changes in [datacenter locations](#). Microsoft does not control or limit the regions from which a customer may access or move customer data.
- **Responding to government requests for data** In the case of government surveillance, Microsoft has taken steps to ensure that there are no "back doors" and no direct or unfettered government access to your data, and Microsoft does not provide any government with its encryption keys or the ability to break its encryption. While we are obliged to respect the laws of countries in which we operate, we are also committed to fight for legal protection of your privacy as a fundamental human right. If a government entity approaches Microsoft directly with a request related to a Microsoft Online Services customer, Microsoft will first try to redirect the entity to the customer to respond. We impose carefully defined requirements for [government and law enforcement requests for customer data](#). We will not disclose data hosted in Microsoft business cloud services to a government agency unless required by law. If we are compelled by law to disclose customer data, we will promptly notify the customer and provide a copy of the request, unless we are legally prohibited from doing so.³ Microsoft [publishes](#) its law enforcement requests report to identify the number and types of requests it receives and its compliance with those requests. Microsoft received permission from the U.S. government to publish information about Foreign Intelligence Surveillance Act orders and National Security Letters.

Global Privacy Information

As a global organization with more than [200 locations](#) around the world, Microsoft is committed to protecting our customers' privacy in every country in which we operate. Our time-tested approach to privacy is grounded in our commitment to give customers control over the collection, use, and distribution of their [data](#).

³ For more information, see [Protecting customer data from government snooping](#).

The following sections include some country-specific privacy information related to Microsoft's cloud services. This whitepaper is a living document, and this section will be expanded in future publications to include additional countries.

Argentina

Argentina has specific, complete, and in-force privacy data protection legislation which is in line with the European model, being the first country in Latin America to achieve an "adequacy" determination for the receipt of EU data transfers. The [Personal Data Protection Act 2000](#) (PDPA, ACT 25,326) protects personal data settled both in public and private databases and registries, granting the privacy and honor rights of the individuals and companies. Other relevant rules contained in PDPA are data owners' consent requirement for the collection, treatment and assignment of personal data; prohibition of secondary use of the information; and prohibition of data transfer to countries that do not offer an adequate level of protection, except for cases in which data subjects give their consent or cases of transfer for data processing purposes with a proper cross-border Data Transfer Agreement (DTA).

Data Processing can be performed without the data owner's consent. However, for this purpose a DTA shall be executed between the database responsible (data exporter) and the data processor (data importer) pursuant to the regulations of the PDPA (Section 25) and the several specifications of the National Data Protection Agency on this matter.

Certain kinds of data (which includes political, philosophical, sexual, and/or religious preferences; ethnical origin; health data; and/or criminal records) is considered "Sensitive Data" whose treatment is as a general principle forbidden under the PDPA, save for very restricted exceptions set forth in Section 7 of the PDPA⁴. If entities are legally authorized to treat sensitive data, they are also legally entitled to contract cloud data processing services.

Data owners have a broad range of rights and actions pursuant their own information. Companies and individuals have the obligation to register their "databases" that contain personal information of individuals in a Database National Register. In case of infringement, sanctions may vary from warnings to significant monetary fines.

The PDPA has been the subject of recent public consultations in advance of the Data Protection Authority's initiative to submit an updated data protection bill for congressional consideration.

Data Protection Authority

[Dirección Nacional de Protección de Datos Personales](#) (DNPDP) is the data protection authority with administrative and audit powers. Save specific exceptions, the PDPA requires written and express data owner consent to transfer personal data. In addition, such data owners shall be informed about the assignment's purpose and the assignee's identity. In addition to the consent required for data collection and its treatment, a different and specific consent is necessary for the assignment of data to

⁴ Treatment for complying with a legal duty, health data treatment by hospitals and health professionals, anonymization of data, treatment of political preferences by political parties, treatment of criminal records by governmental security entities, etc.

a third-party (Section 11 of the PDPA). Both, the assignee and the assignor, are responsible and jointly liable for obtaining said data owner's consent and for compliance of all requirements set forth by the PDPA. Additionally, if personal data is assigned within a foreign assignee, the assignee's country shall provide an "adequate level of data protection." If such country does not provide said protection, the PDPA requires previous and written consent of data owners for the international assignment, otherwise, it is forbidden.

Australia

There is extensive information on the Australian Privacy regulations available on the [Australian Information Commissioner's web site](#). The Office of the Australian Information Commissioner is responsible for administering the [Privacy Act 1988](#). The Privacy Act applies to many organizations in relation to their dealings with personal information, which is defined as "information or an opinion about an individual who is identified or reasonably identifiable." The Privacy Act sets out in Schedule 1 a set of thirteen [Australian Privacy Principles](#) (APPs) which outline how most Australian and Norfolk Island Government agencies, all private sector and non-profit organizations with an annual turnover of more than AU \$3 million, all private health service providers, and some small businesses (collectively, "APP entities") must handle, use, and manage personal information. The Privacy Act does not apply to state and territory public sector health service providers, such as public hospitals.

The following table outlines each relevant obligation under the APPs, and Microsoft's position on each requirement. Microsoft's position is based on the general privacy principles described in this paper.

APP	Summary of Obligations	Microsoft's Position
Open and transparent management principles 1.2	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; thus, the APPs apply in a similarly limited fashion. Microsoft believes the architecture of its online services, supported by contractual commitments, are reasonable steps to ensure that our services comply with the APPs. This is reflected in the certified compliance of Microsoft Online Services to the ISO 27018 Code of Practice . 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 and encryption of data in motion and at rest to support customer compliance.
1.3-1.6	An entity must have a clearly expressed and up-to-date privacy policy containing information about how the entity collects,	Each customer remains responsible for maintaining and making available a privacy policy of its own that complies with the APPs.

APP	Summary of Obligations	Microsoft's Position
	holds, uses, and discloses personal information. An entity must make this privacy policy available free of charge and in an appropriate form.	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 handling policies.
Anonymity and identifier principles 2 and 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.	<p>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.</p> <p>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.</p>
Collection principles 2-5	Outline when an entity can collect personal information. Require that entities which collect personal information make an individual aware of certain prescribed matters.	<p>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.</p> <p>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 our services.</p>
Use and disclosure principles 6 and 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.	<p>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.</p> <p>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 our cloud services is consistent with the APPs.</p> <p>Microsoft supports customer compliance by, for example, facilitating record keeping of all media on which customer data is stored and committing not to use customer data except to provide our services.</p>

APP	Summary of Obligations	Microsoft's Position
Cross-border disclosure principles 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.	<p>The Australian Government's Better Practice Guide, Privacy and Cloud Computing for Australian Government Agencies, states that:</p> <p><i>"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."</i></p> <p>Based on this guidance, Microsoft considers that by using Microsoft's cloud services, a customer will not disclose personal information as Microsoft only processes personal information provided by its cloud customers in accordance with its customer's instructions.</p> <p>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 our cloud services are certified (such as ISO 27001 and ISO 27018) irrespective of where a customer's data is processed. Microsoft also discloses information about data processing on the Microsoft Trust Center, and provides tools that enable customers can find out where their customer data is sent and/or processed.</p> <p>Customers may use this information in obtaining the necessary consents from individuals for transfers of personal or sensitive information.</p>
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.	<p>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 datacenters that are independently certified to ISO 27001 standards and verified by annual compliance audits, which are available for download from the STP and the Service Assurance portal. 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 privacy, security, and integrity of customer data.</p>

APP	Summary of Obligations	Microsoft's Position
		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 correction of, personal information upon request or on their own initiative.

Table 1 - Microsoft's Positions on Australian Privacy Principles

Broadly speaking, the requirements imposed by the APPs are similar to the requirements that are imposed by State and Territory legislation. A summary of the relevant laws and regulators for each State and Territory is listed in the following table.

Jurisdiction	Authority	Legislation
Australian Capital Territory	The Office of the Australian Information Commissioner is exercising some of the functions of the ACT Information Privacy Commissioner. Australian Capital Territory Privacy .	Information Privacy Act 2014 (ACT)
New South Wales	NSW Information and Privacy Commission	Privacy and Personal Information Protection Act 1998 (NSW); and Health Records and Information Privacy Act 2002 (NSW)
Northern Territory	Office of the Information Commissioner for the Northern Territory	Information Act (NT)
Queensland	Queensland Office of the Information Commissioner	Information Privacy Act 2009 (QLD)
South Australia	South Australia has issued an administrative instruction requiring its government agencies to generally comply with a set of Information Privacy Principles and has established a South Australian privacy committee to handle privacy complaints.	Information Privacy Principles Instruction
Tasmania	Tasmanian Ombudsman	Personal Information and Protection Act 2004 (TAS)
Victoria	Victorian Commissioner for Privacy and Data Protection	Privacy and Data Protection Act 2014 (VIC)
Western Australia	Office of the Information Commissioner (WA) .	The state public sector in Western Australia does not currently have a legislative privacy regime. Various confidentiality provisions cover government agencies and some of the privacy principles are provided for in

Jurisdiction	Authority	Legislation
		the Freedom of Information Act 1992 (WA).

Table 2 - Details from <https://www.oaic.gov.au/privacy-law/other-privacy-jurisdictions>

State and Territory Health Privacy

The [Privacy Act 1988](#) (Privacy Act) applies to all health service providers in the private sector throughout Australia. A 'health service provider' is a person or entity who provides a health service and holds health information, even if providing a health service is not their primary activity. Health service providers are covered by the Privacy Act for all activities involving the handling of personal information, not just activities that relate to providing a health service.

The Privacy Act does not apply to state and territory public sector health service providers, such as public hospitals.

Details of the specific State based legislation and regulations are available on the [OAIC website](#).

Brazil

The Brazilian "[Marco Civil de Internet](#)" (Law #12965/12) and the [Decree #8771/16](#) regulate the availability of online services, apps and Internet connectivity in Brazil. It includes Net Neutrality; privacy and data protection; lawful access to data; data retention; connection logs and private communication retention with prompt deletion after expiration of agreed term; requirement of authentication mechanisms to access logs and security. It also sets a data retention obligation, which requires service providers (content, applications, and connection) to retain Internet connection or application access records under secrecy, in a controlled and secure environment, for a period of six months. Microsoft's high standards on privacy and security enable compliance with these regulations.

Reinforcing the commitment to Brazil and the region, Microsoft launched the [Transparency Center in Brasilia](#). The Transparency Center is a high-security location where Microsoft enables governments to review and access the source code of Microsoft products, as well as gain access to important security information. The Transparency Center is designed to foster trust in those products, ensuring transparency and compliance with applicable regulations.

For more than three years, the Brazilian Congress has been debating various national data protection bills. The goal is to set an efficient framework for data protection to address the current challenges in this area. Microsoft supports this important initiative for the country and is actively contributing to this relevant discussion.

Canada

There are several laws in Canada that address privacy rights, and various government organizations responsible for overseeing compliance with these laws. The Federal Privacy Commissioner's Office [notes](#):

"The key factors that determine what laws apply and who oversees them include:

- The nature of the organization responsible for the personal information
 - Is the organization a federal government institution subject to the Privacy Act?
 - Is it a provincial or territorial government institution?
 - Is it a private-sector organization?
 - Is it engaged in commercial activities?
 - Is it a federal work, undertaking or business?
- The location of the organization (where is it based?)
- The type of information (is it personal information, and if so, what type of personal information is it. i.e., is it health information?) "

Federal

The [Privacy Act](#) covers personal information handling by federal departments and agencies and the [Personal Information Protection and Electronic Documents Act](#) (PIPEDA) covers the private sector. The Federal Privacy Commissioner of Canada oversees compliance with the Privacy Act and PIPEDA.

Public Sector Privacy Legislation - Privacy Act This Act imposes obligations on some 250 federal government departments and agencies to respect privacy rights by limiting the collection, use, and disclosure of personal information and provides an individual's right to access and correct personal information held by the Government of Canada about them.

The Privacy Act contains the principles of Collection, Use, Disclosure, Retention, Accuracy and Protection.

Private Sector Privacy Legislation - PIPEDA establishes rules for how private sector organizations may collect, use, or disclose personal information during commercial activities. PIPEDA also applies to federal works, undertakings and businesses in respect of employee personal information. In general, PIPEDA applies to organizations' commercial activities in all provinces, except organizations that collect, use, or disclose personal information entirely within provinces that have their own privacy laws that have been declared "substantially similar" to the federal law.

PIPEDA contains the 10 fair information principles of: Accountability, Consent, Limiting Collection, Limiting Use/Disclosure & Retention, Accuracy, Safeguards, Openness, Individual Access and Challenging Compliance.

Federal Health Privacy Legislation – Generally speaking, there is no specific health information legislation at the federal level. Health information at the federal level is generally treated the same as personal information.

Provincial / Territorial Legislation

Some Provinces and Territories have enacted privacy legislation for the public sector. Several have enacted legislation addressing health privacy, private sector privacy, and personal information

handling by municipal and other government entities. Provincial Information and Privacy Commissioners, and Ombudspersons oversee compliance with provincial legislation.

Provincial Public-Sector Privacy Legislation – Privacy legislation in Canadian provinces generally also includes access to information obligations. The principle of an individual's right to access is included as part of the overarching right to access government information.

British Columbia – The British Columbia [Freedom of Information Privacy Protection Act \(FIPPA\)](#) has a requirement that public bodies *"must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada"* save for a narrow set of exceptions.

Private Sector Privacy Legislation – PIPEDA applies in provinces and territories where no privacy legislation that has been deemed "substantially similar" to PIPEDA has been enacted. British Columbia, Alberta, and Quebec have private sector privacy legislation, deemed "substantively similar" to PIPEDA and as a result the provincial legislation is used in place of the federal legislation. Manitoba has recently enacted private sector privacy legislation that is substantively similar to PIPEDA, but it has not received royal proclamation, and as a result it is not in force.

Health Privacy Legislation – Canada provides publicly funded health care services. Aside from federally operated health programs for indigenous people, the provision of health services is managed at a provincial level. Many jurisdictions across Canada have enacted health privacy legislation regarding the collection, use, and disclosure of personal health information. In most cases, health-specific legislation generally builds upon the existing privacy and security legislation for public sector entities in the province. PIPEDA applies in jurisdictions that do not have specific health privacy legislation or where organizations not subject to public sector legislation handle personal health information.

Personal Information International Disclosure Protection Legislation – Nova Scotia has enacted the [Personal Information International Disclosure Protection Act](#) which, much like the British Columbia legislation, obliges that a *"public body shall ensure that personal information in its custody or under its control and a service provider or associate of a service provider shall ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada"* save for a narrow set of exceptions. One noteworthy exception is for where *"the head of the public body has allowed storage or access outside Canada."*

Municipal Privacy Legislation – Municipal and other local government entities are generally covered under provincial privacy legislation. Ontario and Saskatchewan have legislation that covers personal information handled by municipal and/or local government entities.

Privacy Impact Assessments – The federal government [Directive on Privacy Impact Assessments](#) obliges federal government institutions to initiate privacy impact assessments (PIA):

- when personal information is used for, or is intended to be used as part of, a decision-making process that directly affects the individual;
- upon substantial modifications to existing programs or activities where personal information is used, or intended to be used, for an administrative purpose; and
- when contracting out or transferring a program or activities to another level of government or the private sector results in substantial modifications to the program or activities.

The development of PIAs is mandatory for health information in Alberta and for all public-sector projects subject to the British Columbia [Freedom of Information and Protection of Privacy Act](#). PIAs are recommended practice in the other provinces and territories. Microsoft Canada has commissioned the development of foundational PIAs to assist customers in the development of their own PIAs. These foundational documents are structured as a superset of the PIA templates provided by provinces and federal governments and describe the data flows and legal analysis associated with personal information associated with the use of public cloud services. Customers can request these Foundational PIAs from their Microsoft Canada account team.

Applying Canadian Legislation to the Microsoft Cloud

Private and public-sector organizations that leverage enterprise cloud services for their services delivery always remain accountable for adherence to Canadian privacy legislation. As a result, privacy is a shared responsibility between Microsoft (as a cloud service provider) and the customer using cloud services. At a high level, the customer using cloud services must ensure that they implement solutions to address the principles codified in the public and private sector focused legislation (e.g., Notice, Consent, Accuracy). Customers are obliged to ensure adequate protections and safeguards are used by and within the cloud service provider's environments.

In May 2016, Microsoft [announced](#) the general availability of cloud services delivered from Canadian datacenters located in Quebec City and Toronto. These Canadian datacenters provide data residency for customer data at rest as defined in the [Online Services Terms](#) (OST). Canadian data residency has assisted deployment of cloud services in regions of Canada with data residency requirements.

As Canada does not have local cloud privacy certifications, international certifications, such as ISO 27018, have proven useful in the Canadian context. Former Interim Federal Privacy Commissioner, Chantal Bernier, [indicated](#) the controls over secondary use, the protection of data and the access to information "*supplements domestic law with specific obligations of cloud providers.*"

The [Foundational Privacy Impact Assessments](#) for provide a detailed privacy analysis of using the Microsoft cloud for personal information in the Canadian legislative environment. These assessments reviewed the various customer and service related data flows and analyzed the legal considerations found in legislation, policy and previous findings of the information privacy commissioners.

Finland

Finland has a long culture of strong privacy protection. Privacy and confidentiality of communications is protected by Section 10 of the [Constitution](#). The country is a forerunner even in Europe with over 700 sector-specific acts concerning privacy protection and lawful use of personal data.

Finland has implemented European Directive 95/46/EC on processing, protection and free movement of personal data through Personal Data Act ([523/1999](#)). The act implementing European Directive 2002/58/EC on privacy and electronic communications (the e-Privacy Directive) was combined with other relevant privacy laws into the Information Society Code ([917/2014](#)). An important viewpoint is privacy protection of employees and confidentiality of work-related communications, which are regulated in Act on the Protection of Privacy in Working Life ([759/2004](#)) and in the Information Society Code.

The Data Protection Directive and other pan-EU acts and regulations will be replaced by the GDPR, which will be directly implemented in Finland.

The Personal Data Act requires duty of care, a defined purpose for processing personal data, and exclusivity of purpose, and it lays out general prerequisites for processing, data quality, and documentation of the data processing. Processing of sensitive data (special categories of data) is prohibited except for specified purposes and by specified actors. Processing of Personal Identity Numbers is also regulated.

Using cloud services for storing personal data is generally approved. A customer transferring an existing personal information register to Microsoft cloud does not need to inform the Data Protection Authority ([Tietosuojavaltuutettu](#)) about the transfer. This stems from an Article 29 Working Party [opinion](#) that Microsoft's Online Services Terms are in line with EU Standard Contractual Clause and should not be considered as "ad hoc" clauses.

As there are no provisions in legislation for treating special categories of personal data differently, health care data and other sensitive data can also be stored in the cloud. The DPA guidelines for sensitive personal data require adequate encryption of data at rest and in motion and other sufficient organizational and technical measures to secure the privacy of personal data.

Automated data protection measures

Strict legislation concerning employee privacy in working life requires special consideration when deploying automated data protection measures like Office 365 Data Loss Prevention, Azure Information Protection, Data Governance, and others. The measures need to be planned and documented beforehand, handled with the workforce in established co-operation procedures according to [Act on Co-operation within Undertakings \(334/2007\)](#) in the private sector and respective legislation in public sector organizations. The measures should be executed in a manner that informs and guides employees about proper handling of personal data and that ensures maximal transparency of the automated measures that the service takes on their behalf. When considering

monitoring and reporting options, extra care should be taken to ensure that all planned measures are in accordance with legislation.

Healthcare and Social Welfare Data

The [Act on Electronic Processing of Client Data in Social and Health Care Services \(159/2007, "E-patient Data Act"\)](#) governs the electronic processing of patient data and customer data of social welfare and healthcare customers. The act is applicable to both public and private providers of health care services.

According to the E-Patient Data Act, each IT system used for the processing of patient data must fulfil the material requirements regarding technical interoperability, data security, data protection and functionality ("Material Requirements"). Such requirements are met if the IT system has been designed and manufactured and is operating in compliance with laws and regulations pertaining to data security and data protection and with the national specifications for interoperability. Requirements for functionality are deemed to be met if the IT system is fit for its purpose and can perform the intended operations related to the processing of patient data in compliance with the requirements set forth in the applicable legislation and regulations.

Social welfare and health care IT systems are classified to categories A and B. Class A IT systems include national services maintained by [Kela](#) as well as IT systems which are intended to be connected to these national services directly or indirectly. Other social welfare and healthcare IT systems belong to Class B. Class A IT systems must have a certificate of conformity and Class B IT systems must fulfil the Material Requirements if the system is used on or after January 1, 2017. The [National Supervisory Authority for Welfare and Health](#) (Valvira) maintains a register of approved welfare and health care IT systems. Only IT systems used for social welfare and health care can be recorded in the register.

The [National Institute for Health and Welfare](#) (THL) and Valvira are currently preparing guidelines for using general purpose cloud services and IT systems for handling and storing health care patient and social care customer data. The guidelines should reduce concerns around using cloud services and promote secure use of cloud services, and are expected to be published around mid-2017.

Malaysia

In general, the [Personal Data Protection Act](#) (PDPA) covers all users of personal data and not specific to cloud. In summary, the use of cloud is allowed if it does not prevent the customer from complying with the principles of the PDPA. Customers are also recommended to refer and have documented evidence that they comply with the [Personal Data Protection Standard 2015](#) under the PDPA. Microsoft's cloud services meet and in most cases even exceed the applicable requirements of the PDPA, which maps broadly to many of the requirements included in ISO/IEC 27001 and 27018.

For Financial Services customers, there is an additional need to comply with several guidelines including the outsourcing guidelines that is derived from the [Financial Services Act 2013](#) that is regulated by [Bank Negara Malaysia](#) (BNM). While there is no prohibition on the use of cloud services which meet security and privacy requirements, users of cloud services will need to obtain BNM's

approval for its use as an outsourcing activity. Microsoft has helped several financial services institutions obtain such approval for the use of Office 365.

For the use of cloud services in government, there is no prohibition if the data which is stored meets security and privacy requirements, and is not considered classified data that is governed by the [Official Secrets Act](#). The determination of classified data is defined by the government agencies themselves.

Mexico

The [Mexican Constitution](#) recognizes access to Information and Communications Technologies (ICT) and broadband Internet, as well as protection of personal data, as fundamental rights.⁵ [The Federal Institute of Telecommunications](#) (IFT) and the [National Institute for Transparency, Access to Public Information and Protection of Personal Data](#) (INAI) are the substantive regulators on these fundamental rights, respectively.

National Digital Strategy

Since November 2013, Mexico has had a [National Digital Strategy](#) that includes cloud adoption as one of its goals.⁶ The goals of the National Digital Strategy within the federal public administration are implemented through a set of regulations known as the [ICT Policy](#).

As provided for in the National Digital Strategy, the ICT Policy requires the institutions *"favoring cloud computing to take advantage of scale economies and efficiency of public service, by promoting the use of ICT and open standards, taking into consideration the security of information and protection of personal data."*⁷ Except for information on public security and national security—which requires on-premises processing—the ICT Policy allows institutions of the federal public administration to process any other type of information in the cloud.

Public Sector – Protection of Personal Data

Processing of personal data by public institutions is regulated by the [General Law on the Protection of Personal Data in Possession of Public Institutions](#). This law specifically allows public institutions to process personal information in the cloud. As a prerequisite, it requires that cloud providers have data protection policies equivalent to the legal standards.

"Article 63. Data controller may contract or adhere to cloud services, applications and infrastructure, or other means that imply processing personal information, insofar as the external provider guarantees policies on protection of personal data equivalent to the principles and duties set forth in this law and other applicable provisions on the matter."

"As may be the case, data controller must limit the processing of personal data by the external provider, by means of contractual clauses or other legal instruments."

⁵ Cfr. Art. 6.

⁶ Cfr. Section on Government Transformation, Action Line 3: *"Privilege cloud computing."*

⁷ Cfr. Art. 5, Section I.

In elaboration of the above requirement, the law allows public institutions to contract cloud services only from service providers that meet certain minimum standards, as stated below:

"Article 64. For the processing of personal data in cloud services, applications or infrastructure, or other means in which data controller adheres to them through general contracting clauses or conditions, data controller may only use those services in which the provider:

I. Complies at least with the following:

- a) Has and applies data protection policies consistent to the applicable principles and duties provided for in this law and other applicable provisions;*
- b) Reveals subcontracting involving information on which service is provided;*
- c) Refrains from including conditions which authorize or allow provider to assume title or ownership over information on which service is provided;*
- d) Keeps confidentiality of personal data with respect to which service is provided.*

II. Has mechanisms at least to:

- a) Inform changes to privacy policy and service conditions;*
- b) Allow the data controller to limit the treatment of personal data with respect to which service is provided;*
- c) Establish and maintain security measures for the protection of personal data on which service is provided;*
- d) Guarantee suppression of personal data once the service has been concluded, and allow retrieval of them by data collector;*
- e) Prevent access to personal data to unauthorized persons, or inform any access to data controller if such derives from an order from a competent authority.*

In any event, the data controller may not adhere to services that do not guarantee the appropriate protection of personal data, according to this law and other applicable provisions on the matter."

Public Sector – Archives

As indicated by its name, the General Law on Protection of Personal Data in Possession of Public Institutions deals exclusively with the processing of personal information. However, public institutions may also be subjected to other provisions on processing of information in general, particularly for public archives. Specifically, the Guidelines for the Organization and Conservation of Public Archives [acknowledge](#) the possibility of public institutions to use the cloud to perform their duties on transparency, protection of personal data, administrative procedures, and processing of public archives. In any event, they require the public institutions to make sure that they comply with the applicable legal provisions when using the cloud:

"Thirty-First. Public institutions must assure compliance with applicable law provisions on transparency, protection of personal data, administrative procedures and processing of public archives, in the utilization of collaborative tools and data conservation in cloud services."

The Guidelines provide for general requisites applicable to the contracting of cloud services for the processing public archives:

"Thirty-Second. Cloud services for processing public archives can be used by the public institutions, by taking into consideration the following:

- I. [They must] Guarantee the security of information, and prevent non-authorized access.*
- II. Use data architectural standards that allow the use, conservation and security of documents in the long term, interoperability and personalized metadata schemes;*
- III. The conditions of use of the contracted service must regulate the event of disappearance of the provider with or without prior notice, to avoid the loss of stored information; and*
- IV. The providers must be ruled by the applicable Mexican law, regardless of the geographical location of the servers, or the location of the services provider."*

The use of private clouds is also allowed, although in this case public institutions must comply with additional measures:

"Thirty-Third. Public institutions may process documents in electronic files within a private cloud – a service that is not shared with other parties– by allowing:

- I. The establishment of the concrete conditions of use as for the processing of documents, and responsibility of systems;*
- II. Knowing the location of servers and information;*
- III. The establishment of conditions of use of information according to applicable laws;*
- IV. The utilization of infrastructure for use and private access under control of authorized personnel;*
- V. Custody of sensitive information, and mitigation of security risks through information security policies;*
- VI. The establishment of use of standards and compliance with quality norms for the processing of electronic files;*
- VII. The possibility of integration with applications and internal systems, intranets, institutional websites and other networks;*
- VIII. Reflecting in the system, in an auditable and coherent manner, the policy on processing of public archives and information of the public institutions, and*
- IX. A centralized repository of institutional information."*

All these provisions provide public institutions with full assurance for relying on the cloud for the processing of their information, not only personal data, but other types of information in general.

Private Sector – Protection of Personal Data

Processing of personal data by private institutions is regulated by the [Federal Law on the Protection of Personal Data in Possession of Private Parties](#) and its [Regulations](#). Article 52 of the Regulations allows data controllers to contract cloud services, if it makes sure that cloud provider meets the following minimum standards:⁸

"Article 52. For the processing of personal data in services, applications, and infrastructure in what is called "cloud computing," in which the data controller adheres to the same by general contractual conditions or clauses, such services may only be used when the provider:

I. Complies at least with the following:

- a) Has and uses policies to protect personal data similar to the applicable principles and duties set out in the Law and these Regulations;*
- b) Makes transparent subcontracting that involves information about the service which is provided;*
- c) Abstains from including conditions in providing the service that authorize or permits it to assume the ownership of the information about which the service is provided, and*
- d) Maintains confidentiality with respect to the personal data about which it provides the service, and*

II. Has mechanisms at least for:

- a) Disclosing changes in its privacy policies or conditions of the service it provides;*
- b) Permitting the data controller to limit the type of processing of personal data about which it provides the service;*
- c) Establishing and maintaining adequate security measures to protect the personal data about which it provides the service;*
- d) Ensuring the suppression of personal data once the service has been provided to the data controller and that the latter may recover it, and*
- e) Impeding access to personal data by those who do not have proper access or in the event of a request duly made by a competent authority, so inform the data controller.*

In any case, the data controller may not use services that do not ensure the proper protection of personal data.

For purposes of these Regulations, cloud computing shall mean the model for the external provision of computer services on demand that involves the supply of infrastructure, platform, or software distributed in a flexible manner, using virtual procedures, on resources dynamically shared.

⁸ This same standard is the one replicated in the above-mentioned Article 64 of the General Law on Protection of Personal Data in Possession of Public Institutions (2017). Accordingly, in Mexico both private and public institutions are currently subjected to the same general standards when processing personal information in the cloud.

Regulatory agencies, within the scope of their authority, and assisting the Institute, shall issue guidelines for the proper processing of personal data in what is called "cloud computing."

Telecommunications Industry Specific Provisions

Subject to the above-mentioned prerequisites of Article 52 of the Regulations to the Federal Law on the Protection of Personal Data in Possession of Private Parties, telecommunication service providers may use the cloud to process information. The only exception is made for information required to comply with law enforcement requests, which needs to be processed in-country.⁹ Except for that portion, all other information can be processed in the cloud. On-premises, off-premises, and hybrid solutions are useful to meet this current regulatory requisite.

Morocco

The Kingdom of Morocco enacted [Privacy Act Law 09.08](#) in February 2009, protecting people regarding personal data processing. An independent institution, the [Commission Nationale de contrôle de la Protection des Données à Caractère Personnel](#) (CNDP) was established to control the application of the law and to develop necessary amendments and evolution of the law over time.

The Moroccan law is in most aspects inspired by and equivalent to its European counterparts, the reason being that Morocco has signed [Convention 108](#).

As far as cloud computing is concerned, the Morocco DPA has not yet provided any specific guidance on the use of a public cloud. However, Law 09.08 provides specific provisions regarding, security, outsourcing, and transfer of data outside of the country:

- **Security** The law has strict provisions that require data processors to put in place strict measures to protect customer data. Penal liability is provisioned in law with fines and imprisonment in cases of failure to put appropriate measures in place.
- **Outsourcing** Data controllers must only use subcontractors that provide sufficient guarantees regarding technical and organizational security measures related to the processing of data and must ensure compliance with those measures. Outsourcing must also be governed by a contract or legal act binding the subcontractor to the data controller which includes that the subcontractor acts only under the direction of the data controller and that they are obliged to technical and organizational security measures.
- **Transfer of data outside the country** A provision in Article 43 defines the rules under which data can be transferred. The law allows for data to be transferred to countries that shall ensure a sufficient level of protection of privacy, freedom, and the fundamental rights of individuals with respect to the processing of this data. To that end, the law requires the

⁹ Cfr. Fourteenth Article of the Guidelines on the Collaboration with Law Enforcement Authorities. "Fourteenth. The system or systems used for recording communication data or private lines and lines of fixed and mobile services, must have the capacity of storing and delivering the information required by Article 190, Section II of the Federal Law on Telecommunications and Broadcasting. (...) The systems for processing and storing the databases used by concessionaires or permit-holders to fulfill these obligations, shall be located exclusively in Mexican territory."

DPA (CNDP) to provide the list of such countries, which CNDP has provided through its délibération n° 465-2013.

Nigeria

The Federal Republic of Nigeria does not currently have any personal information data protection legislation. While Chapter 4, Section 37 of the [1999 Constitution of the Federal Republic of Nigeria](#) guarantees the protection of the privacy of every citizen, the Constitution is unclear as to how this guarantee applies to the protection and privacy of citizens' data in the field of ICT. Other than this mention in the Constitution, there is no other legislation covering the protection of the privacy of an individual's data in Nigeria. Certain regulations have been developed by regulators in the ICT industry that provide guidelines on how to protect citizens' data within an information and technology system operated in Nigeria.

One example is the Draft Guidelines on Data Protection published by the [National Information Technology Development Agency](#) (NITDA) in September 2013. The NITDA Guidelines recommend the minimum data protection requirements for the collection, storage, processing, management, operation, and technical controls for information systems deployed within the Federal Republic of Nigeria that are used in processing personal data of Nigerian residents. The NITDA Guidelines applies to public and private organizations that own, use, or deploy information systems for the Federal Government of Nigeria irrespective of whether they are based within or outside Nigeria. The NITDA Guidelines define "personal data" as:

"Any information relating to an identified or identifiable natural person (data subject); information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."

The Guidelines are issued as part of the NITDA Act, so a breach of the guidelines is deemed to be a breach of the Act.

In addition to the NITDA Guidelines, another industry-specific regulation is the General Consumer Code of Practice Regulations 2007 (the "NCC Regulations") issued by the Nigerian Communications Commission (NCC), the regulator of the telecommunications industry in Nigeria. NCC Regulations provide that the collection and maintenance of information on individual Consumers by all Licensees (telecommunications service providers) shall be fairly and lawfully collected and processed, and protected against improper or accidental disclosure. The NCC Regulations further prohibits Licensees from transferring Consumer data (whether Consumer is a Nigerian or foreign citizen) to a third party except as otherwise permitted or required by other applicable laws or regulations.

Nigeria also has no cloud computing regulations, but under section 14.3 of the NITDA 'Guidelines for Nigerian Content Development in ICT' there exists a guideline that mandates all 'Data and Information Management Firms' to host government data locally within Nigeria. While the guideline did not mention anything about personal or private data, the guideline clearly forbids any

government data from being hosted outside Nigeria without the approval of NITDA and the Secretary General of the Federation.

New Zealand

In New Zealand, privacy aspects of the use of cloud services are governed by the [Privacy Act 1993](#). The Privacy Act, which pertains to all personal information collected by either public or private sector organizations, requires that agencies that deal with personal information must do so in accordance with a set of twelve [information privacy principles](#) (IPPs).

The Act makes it clear that the information privacy principles apply regardless of whether personal information is collected, stored, and/or processed overseas or within New Zealand. At the same time, the Act is silent regarding where such personal information may be stored and processed, and regarding what technologies may be used to do this. The net effect is that New Zealand privacy legislation is entirely permissive regarding the use of cloud services, either on-shore or offshore.

To assist New Zealand organizations in understanding whether and how they can use cloud services, the [Office of the New Zealand Privacy Commissioner](#) (OPC) has published an article titled, [What does the Privacy Act say about cloud computing?](#), which includes a cloud computing checklist and a cloud computing guide to making the right choices.

Regarding central government policy regarding use of cloud services, all publicly created and/or held information is governed by the [Official Information Act 1982](#). This legislation establishes the basis for New Zealand government information management frameworks, policies, and practices, including those that relate to the security of government information systems such as the national security classification system. In relation to cloud services, the New Zealand Government has established a “cloud first” policy, which is embedded in [Ministerial decisions about all-of-government ICT strategy](#) and made via the Cabinet decision-making process. As with the Privacy Act, central government policy does not prohibit the use of cloud services for storing or processing personal information. The only prohibition on using cloud services for any purpose whatsoever is in relation to national security requirements. Data held by government that is classified above the level of Restricted is not permitted to be placed in a cloud service. Below that level, the government is actively directing its agencies to adopt public cloud services wherever feasible. Note that this applies not only to core public sector organizations, but also to those in the health and education sectors. Local government is free to adopt cloud services, so long as it abides by the requirements of the Privacy Act in doing so.

When selecting cloud services, government agencies are generally expected to follow a decision-making framework designed and promulgated by the [Government CIO](#) called the [Cloud Computing Risk and Assurance Framework](#). As part of this process, they must undertake a due diligence process focused on security and privacy considerations. Regarding privacy matters, agencies must be clear about the type of data they wish to store and process in the cloud service under evaluation, and how the privacy of personal information can be protected. To assist government agencies in complying with their obligations to robustly evaluate the cloud services they are considering for adoption,

Microsoft New Zealand has published a range of supporting assurance information on the [Microsoft Trust Center](#).

For additional Microsoft resources, please also see:

- The New Zealand section on the Microsoft website, [Navigating Your Way to the Cloud](#).
- Microsoft handbook for New Zealand healthcare organizations - [Navigating your way to the cloud in healthcare – A practical guide for the healthcare industry in New Zealand](#).

Poland

Poland has implemented European Directive 95/46/EC on data protection by the [Personal Data Protection Act of 29 August 1997](#) – Ustawa o Ochronie Danych Osobowych (UODO). This Act and related regulations are fundamental to personal data processing.

The Directive and other pan-EU acts and regulations will be replaced by the GDPR. The GDPR will be directly implemented in Poland and its provisions will be executed from May 25, 2018. UODO will be replaced by the new Data Protection Act, which is under preparation.

Industry-specific provisions (examples)

The personal data processing provisions one can find in:

- The Telecommunication Act regulates data processing and confidentiality, particularly data location, data transmission, message content and personal data;
- The Banking Act regulates how the personal information can be processed under the contract and during negotiations with consumers;
- The Act on Providing Services by Electronic Means (USUDE), which governs the scope of personal data that can be processed by the electronic service provider;
- The Labor Law, which provides rules on the personal data that an employer can request from an employee and from a candidate for employment; and
- The Patient Rights and Patient Ombudsman Law, which governs the rules of maintaining the medical data.

The appropriate regulations are provided to all acts. The list of the local laws is available on the [Inspector General for Personal Data Protection](#) (GIODO) web site.

General Scope of UODO

UODO applies to the following entities when they are residing in the territory of the Republic of Poland or in a different country when they are involved in the processing of personal data by technical means located in the territory of the Republic of Poland:

- State authorities;
- Local government authorities;
- State and municipal organizations;
- Non-government organizations carrying out public tasks; and

- Natural and legal persons and organizations not considered to be legal persons if they are involved in the processing of personal data as a part of their business or professional activity, or for meeting statutory objectives.

Personal data means any information relating to an identified or identifiable natural person (UODO, Article 6). An identifiable person is one who can be identified, directly or indirectly, by reference to:

- Identification numbers; or
- One or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Information is not regarded as personal data if there is required an unreasonable amount of time, cost and manpower to identify the data subject. However, information will be considered personal data if it appears together with other information, which can be related to a specific person.

The rights of the natural persons (data subjects)

The data controller shall provide data subjects with information before collecting the personal data, which includes:

- The identity of the data controller;
- The purpose(s) of data collection;
- The data recipients or categories of recipients, if known at the date of collecting;
- The existence of the data subject's right of access to his data and the right to request the rectification of data; and
- Whether the provision of personal data is obligatory or voluntary (along with information about the legal basis for the obligation, if applicable).¹⁰

The personal data can be collected not directly from data subjects under the conditions described in Article 25.

The data subject has the right to control the processing of his/her personal data, which includes several rights.¹¹ The data subjects' right in this regard does not refer to the personal data which should be amended, updated or corrected pursuant to the principles determined by other laws.

The personal data processing requirements

The data controller should protect the interests of the data subjects with duty of care, and ensure that the data is:

- Processed lawfully;
- Collected for specified and legitimate purposes;
- Not processed contrary to the intended purposes of collection;

¹⁰ UODO, Article 24(1)

¹¹ UODO, Article 32

- Relevant and adequate to the purposes for which it is processed; and
- Kept in a form which permits identification of the data subjects no longer than is necessary for the purposes for which it is processed.¹²

The other obligations of the data controllers include implementing technical and organizational measures, which are appropriate to the risks and category of data, to protect from unauthorized disclosure, falling into the possession of an unauthorized person, processing in violation of the UODO, alteration, loss, damage or destruction.¹³

Consent of Data Subjects

The data subjects' consent is one of the numerous legal basis for processing of the personal data. All the legal basis described in UODO are equivalent and the data subjects' consent is not always required.

There are no requirements regarding the form of consent for processing the non-sensitive data. The online consent is in general sufficient. Written consent (in paper form or by secure electronic signature) is required for the processing of sensitive personal data.¹⁴ Consent cannot be implied or inferred.

Sensitive Data Processing

The following data are considered sensitive:¹⁵

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, religious unity membership, party or trade-union membership, as well as the data concerning health, genetic code, addictions or sex life.
- Data relating to convictions, decisions on penalty, fines and other decisions issued in the court or administrative proceedings.

The processing of sensitive personal data is in general prohibited, unless one of the following applies:¹⁶

- The data subject has given written consent unless the processing involves the deletion of personal data;
- Processing is specifically provided for by a specific provision of another statute and the processor ensures the data is protected by adequate safeguards;
- Processing is necessary to protect the vital interests of the data subject or another person, and the data subject is physically or legally incapable of giving his consent until the appointment of a guardian or curator;

¹² UODO, Article 26

¹³ UODO, Article 36

¹⁴ UODO, Article 27(2)(1)

¹⁵ UODO, Article 27

¹⁶ UODO, Article 27(2)

- Processing is necessary to carry out the statutory objectives of churches and other religious organizations, foundations, and other non-profit-seeking organizations or institutions with a political, scientific, religious, philosophical, or trade union aim; relates solely to the members of those organizations or institutions or to the persons who have a regular contact with them about their activity; and is subject to appropriate security measurements.
- Processing relates to the data necessary to pursue a legal claim;
- Processing is necessary to carry out the obligations of the controller regarding the employment of his employees and other persons, and the scope of processing is provided by the law;
- Processing is required for the purposes of preventive medicine or the provision of care or treatment, where the data is subject to appropriate safeguards and processed by a health professional entity involved in treatment, other healthcare services or the management of healthcare services.
- The processing relates to data which is made publicly available by the data subject;
- It is necessary for scientific research, including the preparation of a thesis required for graduation from university or receiving a degree (the results of scientific research must not be published in a way which allows data subjects to be identified);
- Data processing is conducted by a party to exercise its rights and duties resulting from decisions issued in the court or administrative proceedings.

Security Requirements

The data controller shall implement technical and organizational measures, which are appropriate to the risks and category of data being protected, to protect personal data from:

- Unauthorized disclosure;
- Takeover by an unauthorized person;
- Processing in violation of the UODO; and
- Change, loss, damage or destruction.

The data controller shall:

- Keep documentation describing the method of data processing and security measures;
- Grant authorization to the persons who are processing the personal data;
- Ensure supervision over:
 - what data is entered the filing system;
 - when data is entered the filing system;
 - by whom data is entered the filing system; and
 - to whom data is transferred.
- Keep a register of the persons authorized to process data;
- The controller may appoint the Data Protection Officer (Administrator Bezpieczeństwa Informacji, ABI) who should ensure the compliance with the provisions of UODO.

More precise details on the data processing documentation and technical and organizational conditions, which should be fulfilled by devices and computer systems used for personal data processing, are contained in Regulation from April 29, 2004 issued by the Minister of Internal Affairs and Administration.¹⁷

Processing by the third parties

The data controller can authorize another entity (data processor) by a written contract to process the personal data.¹⁸ The liability for compliance with the UODO remains with the controller.

The data processor can only process data within the scope of and for the purpose(s) determined in the contract. Before processing the personal data, the processor must implement appropriate security measures.

International data transfer

Transferring personal data to another country inside the [European Economic Area](#) (EEA) is treated as local transfer and requires no additional compliance. The transfer of personal data to a third country (outside EEA) can be done only if the destination country ensures an adequate level of data protection.¹⁹

The data controller can transfer the personal data to a third country that does not ensure an adequate level of protection, provided that one or more of the following applies:

- The data subject has given his/her written consent;
- The data subject has wished the transfer;
- The transfer is necessary to perform a contract between the data subject and the controller;
- The transfer is necessary to perform a contract concluded in the interests of the data subject between the controller and another entity;
- The transfer is necessary or required for reasons of public interest or for the establishment of legal claims;
- The transfer is necessary to protect the vital interests of the data subject; and
- The personal data are publicly available.²⁰

The transfer of the personal data to a third country, which does not ensure an adequate level of personal data protection, can be done when GIODO gives prior consent to the transfer.²¹ The GIODO consent is not required when the data controller ensures adequate protection with respect to the privacy, rights and freedoms of the data subject:

¹⁷ UODO, Article 39a

¹⁸ UODO, Article 31

¹⁹ UODO, Article 47

²⁰ UODO, Article 47 (3)

²¹ UODO, Article 48

- EU Standard contractual clauses on personal data protection approved by the European Commission, in accordance with Article 26, paragraph of Directive 95/46/EC;
- Binding Corporate Rules, the legally binding personal data protection principles or policies approved by GODO.²²

Sanctions and Criminal Provisions

In the case of any breach of the UODO provisions, GODO can order compliance with the law by issuing the administrative decision.²³ Furthermore, non-compliance with UODO may be treated as criminal offence and be subject to the financial fine, the partial freedom limitation or up to three years of imprisonment.²⁴

Singapore

Personal Data Protection Act

In Singapore, the privacy aspects of using cloud services are governed by the [Personal Data Protection Act](#) (PDPA). This law governs the collection, use and disclosure of personal data. The PDPA came into effect over 3 phases. The first phase saw the formation of the Personal Data Protection Commission on January 2, 2013. The second phase put into effect the Do Not Call (DNC) Registry which allows individuals to opt out of receiving marketing phone calls, marketing faxes as well as SMS or MMS messages on their Singapore telephone numbers from organizations or businesses. The main personal data protection rules then went into effect on July 2, 2014. This phased approach allowed time for organizations and businesses to review and adjust their policies and practices to comply with the Act.

The PDPA requires organizations to comply with nine main obligations in the PDPA: Consent, Purpose Limitation, Notification, Access and Correction, Accuracy, Protection, Retention Limitation, Transfer Limitation, and Openness. Additional information about the obligations are available on the [Main Advisory Guidelines](#) webpage on the Personal Data Protection Commission's website.

As a technology provider of cloud services, Microsoft is considered a data intermediary for the purposes of the PDPA, as Microsoft processes end-user customer data for and on behalf of its customers pursuant to a written contract. As a data intermediary, Microsoft is only subject to the following obligations under the PDPA:

- **Protection Obligation under Section 24 of the PDPA** – Microsoft protects the personal data in its possession or under its control by making certain security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification and disposal.
- **Retention Limitation Obligation under Section 25 of the PDPA** – Upon expiration or termination of the customer's use of the online service, Microsoft retains customer data stored in the online service in a limited function account for 90 days so that customer can extract the

²² UODO, Article 48 (2)

²³ UODO, Article 18

²⁴ UODO, Article 19

data. After the 90-day retention period ends, Microsoft will disable the customer's account and delete the customer data.

The workings of the PDPA

The PDPA is intended to serve as the baseline standard of protection for personal data. It is also meant to complement sector-specific legislative and regulatory frameworks. This means that in addition to the PDPA, organizations and businesses operating in specific sectors will still have to comply with any laws and regulations that apply to their specific industry.

Scope of the Singapore PDPA

While the PDPA covers personal data, whether in non-electronic or electronic forms, there are provisions in that Act that do not apply to the following 4 areas:

1. For an individual that is acting in a personal or domestic capacity.
2. For an employee of an organization or business acting in the course of his or her employment.
3. For public agencies or organizations that are collecting, using or disclosing personal data on behalf of a public agency. The list of specified public agencies can be found here – [Personal Data \(Statutory Bodies\) Notification 2013](#).
4. Business contact information that includes an individual's name, their position title, business telephone number, business address, business electronic email address or business fax number and other related data about the individual that is not provided by the individual solely for his or her personal purposes.

As described above, there are existing statutes in Singapore, such as the Banking Act, the Insurance Act, that will not be superseded by the PDPA but work in conjunction with these existing statutes. On July 27, 2016, the Monetary Authority of Singapore which regulates the financial services industry in Singapore, issued new Guidelines on Outsourcing that effectively gives the green light for use of public cloud computing services by the financial services industry.

Microsoft Cloud Services compliance

Singapore has developed a common standard for cloud service providers that helps to address customer concerns about the security and confidentiality of data in the cloud, and verifiable operational transparency and visibility to risks to the customer when they use cloud services. This is known as the Multi-Tier Cloud Security (MTCS) Standard for Singapore, and more information about Microsoft's compliance to Singapore MTCS can be found [here](#). One of the requirements of the Singapore MTCS is PDPA compliance, which is covered under the MTCS' Cloud Service Provider Disclosure document in Section 2 Compliance. Because Microsoft Cloud Services, including Azure, Office 365, Dynamics 365, are compliant with MTCS Level 3, and MTCS requires PDPA compliance, all the above-mentioned Microsoft Cloud Services have been certified under MTCS as being compliant with the Singapore PDPA.

South Africa

South Africa's Constitution and other laws govern privacy, including the [Electronic Communications and Transactions Act, 2002](#) (ECTA), and more recently, the [Protection of Personal Information Act, 2013](#) (POPIA).

The South African Constitution's Bill of Rights [states](#) that everyone has the right to privacy which includes the right to not have their person, home or property searched, their possessions seized, or the privacy of their communications infringed. It also [states](#) that everyone has the right of access to any information held by the state and "any information that is held by another person and that is required for the exercise or protection of any rights."

South Africa also has the [ECTA](#), which covers personal information that has been obtained through electronic transactions, which defines a set of rules between the person the information is about and the person/organization ("data controller") who is holding that information. This act states that the data controller must abide by all the following points:

- (1) A data controller must have the express written permission of the data subject for the collection, collation, processing or disclosure of any personal information on that data subject unless he or she is permitted or required to do so by law.
- (2) A data controller may not electronically request, collect, collate, process or store personal information on a data subject which is not necessary for the lawful purpose for which the personal information is required.
- (3) The data controller must disclose in writing to the data subject the specific purpose for which any personal information is being requested, collected, collated, processed or stored.
- (4) The data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law.
- (5) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of the personal information and the specific purpose for which the personal information was collected.
- (6) A data controller may not disclose any of the personal information held by it to a third party, unless required or permitted by law or specifically authorized to do so in writing by the data subject.
- (7) The data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed.
- (8) The data controller must delete or destroy all personal information which has become obsolete.
- (9) A party controlling personal information may use that personal information to compile profiles for statistical purposes and may freely trade with such profiles and statistical data, as

long as the profiles or statistical data cannot be linked to any specific data subject by a third party."

The [POPIA](#) was passed in November 2013. It was a work-in-progress since it was earmarked for implementation by the South African Law Reform Commission in 2005. The delay in its enactment can be attributed in part to the publication of the draft EU GDPR as the POPIA drafting Committee paused to consider some of the proposed innovations in that Regulation. Indeed, it has adopted some of the more radical suggestions, such as mandatory breach notification and the so-called "right to be forgotten."

Application and Jurisdiction of the POPIA

The POPIA provides for a general information protection mechanism applicable to organizations in both the public and private sectors. It will be supplemented by industry-specific and regulator-approved codes of conduct. The eight conditions for lawful processing in the POPIA are largely based on the principles in the 1995 EU Data Protection Directive. An open-ended definition of "personal information" is contained in the POPIA. The definition goes further than its counterpart in the Directive in that it includes information relating to partnerships and companies, and provides a significantly detailed list of examples of personal information. These examples range from private correspondence and information about age, gender and sex through to assignments such as identity numbers, telephone numbers, location information and online identifiers.

The POPIA also defines "special personal information", such as information about criminal behavior and biometric information, which is subject to more stringent conditions for processing. However, there are several exceptions such as the processing of information concerning a data subject's race, so that South African laws which are designed to redress historical racial discrimination are not compromised.

The POPIA does not apply to the processing of personal information during a purely personal or household activity and includes a journalistic exemption where the responsible party is subject to "a code of ethics that provides for adequate safeguards for the protection of personal information".

Processing Requirements of POPIA

Eight data protection conditions, based upon those contained in the Directive, inform the "*conditions for the processing of personal information*" in the POPIA:

1. Accountability
2. Purpose specification
3. Processing limitation
4. Further processing limitation
5. Information quality
6. Openness
7. Security safeguards
8. Data subject participation

Personal data should only be obtained from third parties (rather than the data subject) in limited circumstances such as: consent; where the information is contained in a public record; and where the collection of the information from another source would not prejudice a legitimate interest of the data subject.

Regulation, Compliance and Enforcement of the POPIA

The POPIA establishes an independent supervisory authority, the Information Regulator, with significant powers. These include the power to: authorize a specific breach of the processing of personal information; issue codes of conduct on its own initiative; and issue enforcement notices which, in the case of non-compliance, carry the penalty of a criminal offence. The Information Regulator also has substantial powers to conduct search and seizure operations. The Information Regulator is tasked with the responsibility of regulating and overseeing compliance, receiving and processing data controller notifications, investigating non-compliance, facilitating mediation and conciliation of disputes, and referring non-compliance for prosecution.

A responsible party must take reasonably practicable steps to notify a data subject when collecting personal information, including the purpose of the collection, whether the supply of information is voluntary or mandatory, and whether the responsible party intends to transfer the information to a third country.

The data subject's rights under the POPIA include the right to request, free of charge, whether the responsible party holds personal information about them, as well as a description of the personal information held.

Breach Notification and Right to be Forgotten

Where the responsible party has "reasonable grounds to believe" that data security has been compromised, the responsible party must notify both the Information Regulator and the data subject. Notification must take place "as soon as reasonably possible," but more exact time periods may be delineated in further regulations.

In what may be construed as a "right to be forgotten," a data subject may request the deletion of personal information that is "inaccurate, irrelevant, excessive, out of data, incomplete, misleading or obtained unlawfully." These grounds for deletion are independent of the conditions for lawful processing.

Trans-Border Flow of Information

The POPIA prohibits transfers of personal information outside of South Africa subject to exceptions such as consent or where the recipient is subject to a law, binding corporate rules, or another binding agreement which effectively upholds data processing principles like the conditions for processing of personal information under the POPIA. It is at this stage unclear whether the Information Regulator will require prior approval of data transfer agreements, but from the wording of the POPIA it is doubtful that it will have the statutory power to insist upon such a process.

In some instances, a responsible party must obtain prior authorization from the Information Regulator. For example, permission must be sought for planned trans-border flows of special personal information or personal information of children to a foreign country not deemed "adequate". It is unclear how "adequacy" will be determined and indeed whether it may be assessed independently of the Information Regulator. This may be dealt with in further guidance or regulations.

Cybercrimes

The South African Cybercrimes and Cybersecurity Bill expands on the original sections of the ECTA with the creation of 20 new cybercrime offences. This illustrates the extent to which technology is being used for unlawful purposes and the need to protect yourself in your activities online.

Existing Cybercrimes

There are currently only three cybercrime offences in the ECTA:

1. Unauthorized access to, interception of or interference with data;
2. Computer-related extortion, fraud and forgery; and
3. Attempting and assisting others to commit the above offences.

Penalties on conviction include fines (of unspecified amounts) and imprisonment of up to 12 months or five years, depending on the severity of the offense.

Newly Proposed Cybercrimes

The Bill gives further detail to the ECTA offences and criminalizes activities relating to:

- Use of personal and financial information to commit offences;
- Use of hardware, software and computer systems to commit offences;
- Prohibited financial transactions;
- Hacking;
- Possession and distribution of malware;
- Terrorism, espionage, extortion and appropriation;
- Hate speech, discrimination and violence; and
- Infringement of copyright.

Taiwan

The [Personal Information Protection Act](#) (PIPA) is the major law covering personal information protection and privacy, and it applies to both the public sector and the private sector. The PIPA was enacted to govern the collection, processing and use of personal information to prevent harm to individual rights, and to facilitate the proper use of personal information. Violation of the PIPA will lead to criminal, administrative, and/or civil liabilities under the PIPA. Customers from certain industries, such as financial institutions, insurance companies, or healthcare institutions, might be subject to additional regulations. However, these additional regulations just provide specific guidelines for certain industries to comply with the PIPA rather than creating obligations in addition the PIPA.

For customers of financial institutions and insurance companies within the territory of Taiwan, the use of Microsoft Cloud Services may trigger the application of the Directions Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operations. In general, Microsoft does not on its own initiative collect, process or use personal information provided by customers, and does not have control of or own such personal information. Microsoft customers are the owners of such data and Microsoft uses the customers' data only for purposes consistent with providing Microsoft Cloud Services to the customers in accordance with the applicable agreement (mainly, the Microsoft Online Services Terms). Therefore, the relevant policies and commitments of Microsoft Cloud Services meet the requirements of the abovementioned regulations and the PIPA, though how these regulations and the PIPA should be applied may be still under debate. For additional information, see the [Regulations Governing Internal Operating Systems and Procedures for the Outsourcing of Financial Institution Operations](#) and the [Directions for Operation Outsourcing by Insurance Enterprises](#).

Thailand

Thailand does not have a unified comprehensive personal data protection regime and laws governing cloud computing. The protection of privacy rights of individuals is currently regulated by:

- The Constitution, which recognizes the right to privacy;
- The Thai Civil and Commercial Code, which provides personal data protection under the wrongful act principle;
- Statutory laws in some specific areas, such as banking and financial services; and
- The Official Information Act B.E. 2540, governing the government's collection and maintenance of personal data.

Thailand also has specific requirements for various sectors.

- **Financial Services:** The Ministry of Finance and the Bank of Thailand (BOT) have issued regulations with respect to outsourcing by FSIs. In brief, an FSI must arrange to have a contract in writing kept at the FSI for inspection by the BOT. The regulations also lay out various topics that must be included in the contract, including a requirement to address protection of data/information.
- **Healthcare:** The law provides generally that personal health information must be kept confidential, and that no person may disclose it in such a manner as to cause damage to the data subject. Accrediting bodies may impose requirements that are more specific and more stringent.
- **Public Sector:** Public procurement rules would apply, as would the Official Information Act B.E. 2540 and the Rule on Maintenance of Official Secrets B.E. 2544. The applicable regulator(s) of public-sector bodies would vary, depending on the public-sector body. Some public-sector bodies are effectively self-regulating. The Official Information Commission has certain authority with respect to information of State enterprises. If a State enterprise collects or maintains personal information, it is subject to additional privacy requirements including in

respect of consents from data subjects and data security. The Ministry of Finance and the Bank of Thailand have issued regulations with respect to outsourcing by FSIs. In brief, an FSI must arrange to have a contract in writing kept at the FSI for inspection by the Bank of Thailand. The regulations also lay out various topics that must be included in the contract, including a requirement to address protection of data/information.

Bank of Thailand Outsourcing Policy and IT Outsourcing Policy

The BOT has specific guidelines that anticipate and permit the use by regulated entities of outsourced IT services such as cloud computing. Different notification and approval requirements apply depending on which activities are being outsourced and how those activities are categorised under (i) Outsourcing Policy; and (ii) IT Outsourcing Policy.

Outsourcing Policy

Pursuant to the Outsourcing Policy, there are three umbrella types of activity:

- Material (activities that if disrupted would greatly impact the FSI);
- Non-material (activities that support the operation of the bank, including activities such as document storage); and
- Low-risk (activities such as cleaning services).

Within “material”, activities are either:

- “Strategic functions”, which relate to decision-making aspects of the FSI's business, which may directly affect the capital, income or profit of the business), in which case they cannot be outsourced at all except in limited circumstances and even then, on a case-by-case basis as approved by BOT, or
- “Non-strategic functions”, which are functions not related to the strategy of the institution, but which support the strategy, such as finance and accounting), in which case they can be outsourced but only with BOT approval for the use of offshore datacenters.

If activities are non-material or low-risk, no notification or approval requirement applies. It seems safe to assume that low-risk activities are not relevant for the purposes of Microsoft Cloud services and the use of Microsoft Cloud Services would in most cases fall into either material or non-material activities, so it is likely that FSI customers will want to consult with the BOT.

IT Outsourcing Policy

Where the services constitute a critical IT outsourcing under the IT Outsourcing Policy, 30-days' notice to BOT is required for private cloud services while 30 days' advance approval of BOT is required for public cloud services, prior to the commencement of, or change to, the outsourcing. Critical IT outsourcing means IT outsourcing that may cause risk and widespread effect on the FSIs or other damage or incidents. Examples of critical IT outsourcing are core banking, datacenter, and network. It is very likely that the use of Microsoft cloud services would be considered “critical.”

BOT Notification 19/2559, which replaced BOT Notification Sor Nor Sor 6/2557 on IT Outsourcing in January 2017, expands and clarifies the types of outsourcing activities allowed by BOT.

Microsoft Privacy Resources

Listed below are some of the privacy resources available from Microsoft:

- [Brad Smith blog post - Our search warrant case: An important decision for people everywhere](#)
- [Brad Smith blog post - Responding to government legal demands for customer data](#)
- [Building Global Trust Online, 4th Edition: Microsoft Perspectives for Policymakers](#)
- [Cloud Privacy at Microsoft](#)
- [Cortana and Privacy](#)
- [EU Policy blogs from Microsoft on Privacy](#)
- [John Frank blog post - EU-U.S. Privacy Shield: Progress for privacy rights](#)
- [Microsoft Azure Legal Information](#)
- [Microsoft Dynamics 365 Privacy](#)
- [Microsoft Intune Privacy Statement](#) and [Microsoft Intune Privacy Information](#)
- [Microsoft Online Services Privacy Statement](#) and [Microsoft Online Services Terms](#)
- [Microsoft Online Subscription Agreement](#)
- [Microsoft Privacy Practices](#)
- [Microsoft Privacy Statement](#)
- [Microsoft Transparency Hub - Law Enforcement Requests](#)
- [Microsoft Trustworthy Computing](#)
- [Microsoft.com Privacy Statement](#)
- [Privacy Guidelines for Developing Software Products and Services](#)
- [Privacy Models](#)

Summary

Microsoft recognizes that privacy and security are major concerns for cloud customers, and we develop our products and services from the ground up with privacy and strong data protection in mind. Microsoft's privacy principles and privacy standards guide the collection and use of customer and partner information at Microsoft and give our employees a clear framework to help ensure that we manage data responsibly. The Microsoft Corporate Privacy Policy comprises six key privacy principles for the protection and appropriate use of customer information, such as information submitted by customers, data obtained from third parties, and data that is automatically collected.